

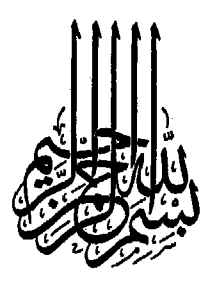
دليل الوقاية من فيروس الحواسيب

تأليف: رونالد ميكلين

ترجمة: مركز التعريب والبرمجة



دليل الوقاية من
فيروس الحواسيب


بسم الله الرحمن الرحيم

دليل الوقاية من
فيروس الحواسيب

تأليف: رونالد ميكلين



ترجمة: مركز التعريب والبرمجة



الطبعة الأولى

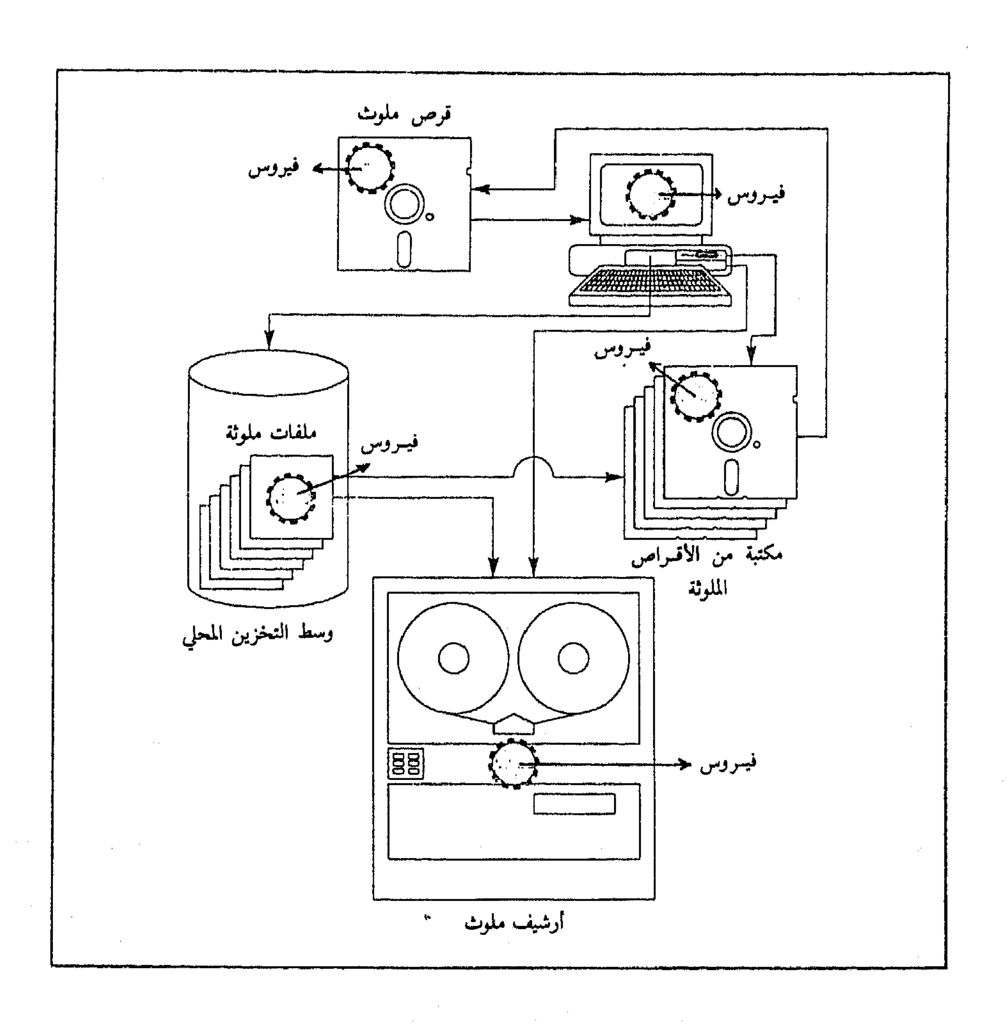
1412 هـ ـ 1992 م



الدار العربية للعلوم
Arab Scientific Publishers
هاتف 811373-811385-806983 ـ ص.ب 5574-13
تلكس ABJAD 21583 LE — KHATAB 21713 LE
فاكس 961-1-860138 ـ بيروت ـ لبنان

محتويات

مقدمة 7
الفصل الأول: فيروسات الحواسيب ــ خطر عالمي 11
الفصل الثاني: كيف يجعل الفيروس الحاسوب مريضاً 20
الفصل الثالث: الأسئلة العشرون الأكثر تداولاً بخصوص فيروس الحاسوب . . 29
الفصل الرابع: أمثلة على بعض الفيروسات 47
الفصل الخامس: الفيروسات ليست سبب المشاكل دائماً 49
الفصل السادس: ما العمل عند وجود الفيروس 62
الفصل السابع: وقاية المعطيات ومنع عدوى الفيروس 78
الفصل الثامن: المجموعة الدولية من أشقياء الحواسيب الفيروسيين 95
الفصل التاسع: تأثير الفيروس على مستقبل الحوسبة 113
الفصل العاشر: عندما يهجم الفيروس أو تزلزل الأرض باشر تنفيذ خطة للكوارث 130



قرص ملوث
فيروس
فيروس
فيروس
ملفات ملوثة
فيروس
مكتبة من الأقراص الملوثة
وسط التخزين المحلي
فيروس
أرشيف ملوث

مقدمة

هنالك بعض البراجيات الشريرة التي تحاول السيطرة على حاسوبك. وهذا الكتاب يحذرك ويبلغك عن الأساليب والأسلحة التي تُستعمل لمهاجمة نظامك ويبلغك كيف تحمي معطياتك وكيف ترد الهجوم.

إن **دليل الوقاية ضد فيروس الحواسيب** هو عبارة عن محاضرة مكثفة في التخطيط للحالات الطارئة. وهو يحتوي على المعلومات الأساسية التي يجب أن يلم بها جميع من يستعمل الحواسيب أو مدراء المشاريع التي تعتمد على معالجة المعطيات بالنسبة لفيروسات الحواسيب.

وخطر الفيروس لا يقتصر على نوع من الأنظمة بل قد يدخل إلى أي نظام. وخلال قراءة هذا الكتاب سوف يتضح لك مدى الخطر المحدق بنظامك وكيف تخففه بشكل كبير. وسوف تتعلم ما هي البراجيات الشريرة ولماذا تم تصميمها وكيف تخرق الأنظمة البريئة. وسوف تتعلم كيف تدافع عن حاسوبك ضد هجوم الفيروس. والنصائح المذكورة تساعد أيضاً على التعامل مع الحالات الطارئة الأخرى المتعلقة بمعالجة المعطيات بدءاً بالزلازل ووصولاً إلى القهوة المنسكبة.

وفهم المعلومات التي يتضمنها هذا الكتاب لا يحتاج إلى خلفية تقنية خاصة. والموضوع المطروح مثير للاهتمام بحد ذاته ولذا بغض النظر عما إذا كنت مدير شركة أو مستعمل عادي فسوف تجد متعة وفائدة عند قراءة هذه الفصول.

وإذا كنت معنياً بحماية أحد المشاريع التجارية أو المؤسسات من خطر الفيروسات فإن معلومات هذا الكتاب تساعد على تحفيز وتنوير الموظفين وزملاء العمل. يمكن على سبيل المثال استعمالها كأساس لنظام معلومات خدماتي حول فيروس الحواسيب خاص بالشركة واعداده بحيث يتلاءم مع مستلزمات كل شركة على حدى. ويمكن الدمج ما بين نظام المعلومات الخدماتي وخدمة دعم المستعمل للبرامج التطبيقية مثل معالجة المعطيات أو قواعد المعطيات. وهذا يتناسب بالأخص عند حصول تغييرات دائمة في الموظفين أو عند الارتقاء إلى إصدار أجدد

للبرامـج مـع وجود متطلبات تدريبية معينة. ويستطيـع هذا الكتاب أيضاً توفير مواد لمقررات الشركات لإعداد محاضراتها وبرامـج تدريبها الداخلية.

الخطر حقيقي

إن فيروس الحواسيب هو خطر حقيقي يهدد سلامة مجتمعنا. والكثير من الحكومات والقطاعات التجارية بـدأت تعترف بحقـائق هذا المرض المعدي. ويحـذر المعهد الـوطني للمواصفات القياسية والتقانة NIST في وزارة التجارة الأميركية في نشرته الخاصة تحت عنوان «فيروسات الحواسيب والمخاطر المترتبة: دليل إداري» من أن: «الخطر متنوع ومختلف وقد يكون جسيم إلى حد يتطلب إعادة تركيب وادخال كامل لجميـع براجيات ومعطيات النظام. وبسبب سرعة انتشار الفيروسات إلى برامـج وانظمة أخرى فإن الضرر قد يتضاعف بشكل هندسي».

لقد قامت مجلـة Computerworld التي تتناول مواضيـع إدارة أنظمة المعلومات بمقارنة سرعة تأثر أنظمة الشركات والحكومات بناقلات النفط التي تهدد في أية لحظة بالارتطام والتسبب بكارثة تؤدي إلى عواقب رهيبة. ولقد حذرت هذه المجلة في عددها الصادر في 26 آذار (مارس) 1990 تحت عنوان «Lax security invites liability nightmare» بأن مدراء أنظمة المعلومات قد يتعرضون للملاحقة القانونية كما حصل مـع قبطان الناقلة Exxon Valdez الذي وجهت إليه تهم جنائية. وفي حالة المدراء فإن التهمة سوف تكون «الإخفاق في حماية أنظمة حواسيب شركاتهم ضد هجوم المخربين والفيروسات وغيرها من الخروقات الأمنية».

ويضـع بعض الخبراء هذا الخطر في مرتبة عالية بحيث يؤمنون بأنه لو فهم المدراء مقدار الخطر المحدق بمعطياتهم واحتمال خسارتهـا والدعاوى القانونية المترتبة عن ذلك فإنهم سوف بوقفون شبكات حواسيبهم فوراً.

إذا لم تكن قد اختبرت شخصياً حالة عدوى فيروسي على حاسوبك فإن الواقـع الاحصائي للنمو الهندسي لمعدل العدوى يشير إلى أنك سوف تتعرض له قريباً. فالحجم الكبير للضغوطات الفيروسية المنتشرة حالياً والتي تزيد عن 80 نوعاً يعني بأن المخاطر المحدقة بالأنظمة وبالأخص تلك المرتبطة ببعضها البعض عبر شبكات اتصال سوف تتصاعد وتتزايد.

ولذا من المهم بالنسبة للأفراد وللمؤسسات الذين تهمهم الحوسبة تبني سياسة شاملة ومنسقة لحماية انظمتهم ضد عدوى الفيروس والتمكن من القيام بعمل فعال في حال حصول عدوى.

لا حاجة لأن تكون خبيراً لتتمكن من وقاية نظامك

لا يجب أن تكون خبيراً في الحواسيب لتفهم هذا الكتاب أو لاكتساب المعرفة المطلوبة للتحكم بأعمال الحوسبة التي تخصك. وقد صمم هذا الكتاب بشكل خاص لدعم حقك الأساسي في عدم وجوب فهم طريقة عمل الحاسوب والبرنامج لتتمكن من الاستفادة من هذه التقانة الرائعة.

معظم الأشخاص لا يرغبون بأن يصبحوا مبرمجين. وجل ما يبتغونه بكل بساطة هو جعل الحواسيب تعمل لمصلحتهم كما الحال مع السيارات والثلاجات واجهزة التلفزة التي تعمل دون أن تتطلب معرفة تصميمها الهندسي. ولكن الآلات التي تساعدنا على إدارة المعلومات تتطلب من المستعمل علاقة أكثر قرباً وتعقيداً. ولا نستطيع إبعاد أنفسنا بالكامل عن فهم القواعد الأساسية لكيفية عمل تلك الآلات والأسباب وراء حالات العمل السيئة.

ولكن حالما تقرأ الفصول الأولى التي تصف أسس نشوء وانتشار الفيروس سوف تصبح قادراً على اختيار استراتيجية دفاعية على أساس احتياجاتك الخاصة. وقد تقرر عدم القيام بأي عمل وقبول المخاطرة المحتسبة. وهذا حقك ولكن أتمنى أن تستخلص في النهاية بأن هذه الأعمال لها مردودها. وفي الواقع وبقليل من الجهد تستطيع تخفيض خطر العدوى بمقدار 95 بالمئة أو أكثر وتعزيز فرص استعادة المعطيات المفقودة في حال وقعت ضحية الفيروس. ومعرفة هذه الوقائع مهمة وقد جمعناها في هذا الكتاب بحيث تستطيع بعد بضعة ساعات معرفة كل ما تريد معرفته حول فيروسات الحواسيب.

جولة قصيرة على الفصول

تعطيك الفصول الأولى من هذا الكتاب معلومات عن عدوى الفيروس. وسوف تتعلم عن مدى حدة هذه المشكلة وكيف تؤثر الفيروسات على نظام الحاسوب وتحصل على أجوبة على بعض الأسئلة الشائعة حول الفيروس.

يعطي الفصل الرابع أمثلة عن بعض الفيروسات الشائعة ويبين الفصل الخامس بأن حاسوبك قد يتصرف بغرابة لأسباب لا علاقة لها بعدوى الفيروس. وهنالك العديد من عوارض الهجوم الفيروسي المماثلة لعوارض تنتج عن مشاكل من العتاد (Hardware) أو البراجيات (Software) وهذا الفصل يعطيك ملاحظات تساعدك على معرفة الفرق.

إذا التقطت فيروساً فإن الفصل السادس يشرح لك الخطوات الواجب إتباعها للخروج من المأزق. وبإتباع إجراءات ذلك الفصل سوف تتمكن من العمل بسرعة وبذكاء لتخفيف الضرر الناتج عن هجوم فيروسي إلى أقصى حد.

والاستراتيجية الفضلى هي الوقاية بالطبع. يعطيك الفصل السابع نصيحة عملية حول طريقة حماية ووقاية المعطيات بما في ذلك نظرة أقرب على بعض عادات الحوسبة الخطيرة التي قد تفتح الباب لهجوم فيروسي أو لمشاكل أخرى في الحاسوب.

ويقدم لك الفصل الثامن أشقياء عدوى الفيروس. وسوف تتعلم خصائص **قاتل الأقراص** (Disk Killer) و**المنتقم الأسود** (Dark Avenger) و**القدس** (Jerusalem) والفيروس الشهير **يوم كولومبس** (Columbus Day) وغيرها.

ويبين الفصل التاسع كيف قد تغير عدوى فيروس الحواسيب أسلوب الحوسبة في المستقبل.

إذا لم تكن تملك خطة جاهزة للكوارث في حال حصول هجوم فيروسي أو حتى لحالات الكوارث الطبيعية. فإن الفصل العاشر يبين لك كيف تفعل ذلك. وسوف تتعلم كيف تحدد المعطيات المهمة فعلياً وكيف تحميها في حالة الأزمات وكيف تسترد عمليات معالجة المعطيات بأدنى حد من الانقطاع.

تؤلف المعلومات المذكورة في هذا الكتاب مجموعة أدوات شاملة تساعدك على تجاوز مشكلة عدوى الفيروس. ولقد كان أحد مواضيع الثورة المعلوماتية هو أن المعرفة مرادفة للقوة. ويوجد في هذا الكتاب المعرفة التي تساعدك على اكتساب القوة المطلوبة لمحاربة خطر الفيروس الذي يهدد نظامك.

1 فيروسات الحواسيب - خطر عالمي

إن العديد من الأشخاص حتى الآن لا يأخذون فيروسات الحواسيب على محمل من الجد. والسبب الرئيسي هو الجهل يتبعه شعور اللامبالاة والعادات. وهنالك بعض القطاعات التجارية في مجال صناعة الحواسيب التي لا تريد التركيز على هذا الخطر المحدق بمستقبلنا التقني والتي حاولت إنطلاقاً من خوفها حيال رد الفعل السلبي على منتوجاتها وخدماتها، بذل أقصى جهدها للحؤول دون حصول نقاشات عامة عن هذه الظاهرة التي تشكل خطراً على جميع النشاطات تقريباً في مجتمعنا الحاضر الذي يعتمد على الحواسيب.

وهنالك أيضاً العديد من مختصي الحواسيب والأمان الذين لم يفهموا بسرعة ماهية الفيروسات ولماذا أنشئت وما هو خطرها. والخبرة في الحوسبة قد تكون في الواقع العائق في وجه الفهم المبدئي للخبير التقني لهذه الظاهرة وذلك لأن الفيروسات هي مفهوم لم يكن بالإمكان تحليله إطلاقاً خلال التدريب على الحاسوب أو عند تصميم وتشغيل الأنظمة. ولطالما كانت الحوسبة والأمان في الأيام ما قبل الفيروسات أموراً منطقية، ولم يكن هنالك مكان للنشاطات الحقيقية التي قد تتعرض لحالات غير متوقعة مثلما الحال مع قطاع الطب. ولهذا السبب، فحتى مهندسي البراجيات وخبراء الأمان ذوي الخبرة عانوا من مشكلة في التأقلم مع البرامج الفيروسية عندما ظهرت لأول مرة.

خلال حرب القرم جاهدت مُؤسِّسَة فن التمريض الحديث، فلورنس نايتنغايل، لإقناع الجراحين العسكريين ذوي الخبرة بأن مرضاهم يموتون بهذا العدد الكبير لأن الجراحين لا يقومون بتطهير أيديهم وادواتهم بشكل جيد ما بين العمليات الجراحية مما أدى إلى انتشار أمراض معدية فتاكة. وهذا المثال التقليدي للصعوبات التي تواجه المرء عند محاولة التغلب على الأفكار المترسخة للخبراء تعكس ما يحصل اليوم في حقل صناعة الحواسيب.

ولقد استغرق إقناع خبراء الحواسيب الكثير من الوقت عن الحاجة لإبقاء أدواتهم الإلكترونية نظيفة. وامثال فلورنس نايتنغايل في عالم الحواسيب الذين أطلقوا التحذيرات حول

مخاطر الفيروسات في الأيام الأولى مثل البروفسور فرد كوهن الذي حدد الإسم **Computer virus** أو فيروس الحاسوب للإشارة إلى البرامج الذاتية التناسخ (Self-replicating)، ومهندس البرامجيات جون ماكافي العامل في سيليكون فالي في الولايات المتحدة والذي أسس الجمعية الصناعية لفيروس الحواسيب CVIA، جوبهوا بالشك من قبل قسم كبير من قطاع صناعة الحواسيب. والآن إذا قرأت العدد الكبير من الرسائل الموجهة إلى الجمعية CVIA من ضحايا الفيروس فإنك تدرك بأن ماكافي قد أضحى بطلاً للعديد من الأشخاص بسبب التحذيرات والمساعدة التي يعطيها.

ولقد جوبهت شخصياً أيضاً برد فعل سلبي عندما حاولت كمستعمل للحاسوب وكاتب استقصائي التحذير عن الخطر المحدق. ولقد تعثر كتابي الأول الذي حاولت تحضيره عن موضوع الفيروس بالتعاون مع خبير في أمان الحواسيب لأن المؤلف المساعد لم يصدق بأن التوقعات المزعجة التي أطلقها هي توقعات حقيقية وواقعية. وفي الواقع من الصعب الآن تجسيد الحجم الحقيقي للأذى الكبير الذي تلحقه الفيروسات.

وحتى في أواخر العام 1989 فقد قوبلت بالشك من قبل جمهرة من المدراء خلال مؤتمر لصناعة الحواسيب عندما قلت بأن البائعين العاملين لدى شركاتهم ينشرون عدوى الفيروس باستعمال أقراص العروضات في آلات الزبائن. والآن، وبعد أن تعرض بعض من أفضل زبائنهم إلى حالات عدوى متعددة نتيجة لهذا العمل، فإنهم يأخذون هذا الوباء على محمل من الجد.

ولم يقم الكتاب الخبراء بموضوع الحوسبة والذين نعتمد عليهم لإطلاعنا على آخر التطورات المهمة بعمل جيد لناحية تغطية موضوع الفيروس. وكثيراً ما يأخذون برأي أولئك الذين لهم مصالح تجارية والذين يخففون دائماً من حجم خطر الفيروس بسبب الضرر الذي قد يلحقه بالمبيعات.

وبقراءة هذا الكتاب تكون قد أظهرت رغبة حقيقية بأنك تريد الاطلاع على موضوع الفيروس. وفي الواقع فإنك إتخذت الخطوة الأولى نحو منع نظامك ومعطياتك من اللحاق بضحايا عدوى الفيروس. وتواجه أغلبية الحواسيب خطر كبير في التقاط عدوى فيروس الحواسيب في وقت من الأوقات ولكن في الصفحات التالية سوف تتعلم كيف تتعرف على علامات الخطر والقيام بعمل فعال لمنع خطر العدوى أو تخفيفها إلى أدنى حد. وتستطيع بهذه الطريقة وقاية نظام حاسوبك وبنفس الوقت متابعة التمتع بالمساعدة الهائلة التي يوفرها وذلك بغض النظر عما إذا كنت تعمل ضمن نظام شركة كبير أو تحاول الإنطلاق مع حاسوبك الشخصي الأول.

مشكلة الفيروس تتفاقم

لقد شهدت السبعينات تطوراً سريعاً للحواسيب التي تمثل التقانة الأكثر حداثة ودلالة منذ اختراع العجلة. وفي الثمانينات أشرق عصر المعلومات واصبحت قدرة معالجة المعطيات الإلكترونية في متناول الأشخاص العاديين.

> قدرتنا الجديدة على معالجة المعلومات واستعمال الآلات بطرق تحسن كثيراً من نمط حياتنا هي عرضة للهجوم.

كلما ازداد اندماج هذه التقانة في حياتنا اليومية فإن التسعينات قد تكون الحقبة التي سوف نقاتل فيها لاستعادة سيطرتنا عليها. وقدرتنا الجديدة على معالجة المعلومات واستعمال الآلات بطرق تحسن كثيراً جداً من نمط حياتنا هي عرضة للهجوم من قبل الأشقياء ومحبي المداعبات السمجة والمخربين والمجرمين ومهووسي المجتمع.

ولقد بدأ هذا العقد من الزمن بداية سيئة فبينما بدأ المسؤولون السياسيون ورجال الأعمال باتخاذ الإجراءات لمكافحة هذا الخطر ارتفعت عدوى الفيروس في الحواسيب إلى ما فوق 2 مليون علامة حسب تقديرات الجمعية CVIA. وهنالك ضغوطات جديدة من الفيروسات الشريرة قادرة على إتلاف وتخريب المعطيات يجري إنشاؤها ونشرها في جميع أنحاء العالم. وقدرتنا على التحكم بالحواسيب تجابه أكثر وأكثر نتيجة ظهور فيروسات قادرة على الطفر (mutation) بحيث تؤقلم نفسها مع جميع البيئات الغريبة كما تفعل الفيروسات البيولوجية.

لقد اتُّهمت بنزعتي إلى المبالغة والتشاؤم الزائد حول الأذى الذي بإمكان الفيروس إلحاقه. وأشجع القارىء على تقييم وجهات نظري ليس فقط بالمقارنة مع وجهات نظر أولئك الذين يحاولون إقناعك بعدم أخذ الفيروس على محمل من الجد، بل مع الإثباتات الرسمية لخطر فيروسات الحاسوب الموجودة في المستندات العامة التي ينشرها مجلس الشيوخ الأميركي.

لقد استعمل أحد الشهود التعبير «الإرهابيون استولوا على الطائرة!» لوصف القضية المعروضة على اللجنة الفرعية القضائية التابعة لمجلس الشيوخ الأميركي المختصة بفيروسات الحواسيب والتي بدأت تجمع الاثباتات في العام 1989.

«مقدرة الفيروسات على إلحاق الضرر كما اثبتته الحالات الأخيرة كبير جداً والكلفة المترتبة هائلة،» هذا ما اخبرته الشاهدة الخبيرة كارولين كون للّجنة وهي تمثل 10,000 عضو في جمعية مدققي الحسابات لأنظمة المعالجة الاكترونية للمعطيات EDPAA وهي مجموعة دولية من خبراء أمن الحواسيب. وقد أدلت كون في جلسة اللجنة الفرعية لمجلس الشيوخ بالبيان التالي:

لقد كلفت الفيروسات الوكالات الحكومية والمعاهد التربوية ملايين الدولارات لمنع هجوم فيروسات الحواسيب واكتشافها والتعافي منها. ولدى الفيروسات القدرة على إتلاف أو تعطيل أنظمة الحواسيب والشبكات التي توفر وسائل اتصال حيوية ودعماً معيشياً مثل خدمات الهاتف للاتصال المحلي أو البعيد ومرافق الإطفاء والشرطة والطوارىء والاتصالات العسكرية ووسائل التبادل المالي وأنظمة ضبط حركة الطيران.

وقد شددت على أنه بالرغم من هجوم الفيروسات على القطاعات التجارية والحكومية والعلمية والتربوية فإنه من المستحيل قياس مدى استفحال العدوى بدقة وذلك لأن العديد من المؤسسات والوكالات الحكومية تتستّرعلى هذه الهجومات خوفاً من إظهار مدى ضعفها وتجنباً للدعايات المغرضة.

«يتضح بأن التقارير حول هذا الموضوع ضئيلة جداً إلى حد دراماتيكي،» هذا ما قاله رئيس اللجنة الفرعية شارلز شومر مشيراً إلى أن بعض أنظمة زملائه في مجلس الشيوخ قد تعرضت للعدوى. ولقد حاول جاهداً الحصول على تقييم كمي لحجم المشكلة ولكن عدم توفر التقارير يجعل الشهود الخبراء يعطون تقديرات غير واقعية لمئات الآلاف من حالات العدوى.

والموضوع الأكيد هو حصول ازدياد مضطرد في حالات العدوى. وقد لاحظت الجمعية EDPAA زيادة من عشرة أضعاف ما بين الشهر الأول من العام 1988 والشهرين الأخيرين. ولهذا السبب قدرت الجمعية CVIA بأن معدل العدوى ازداد مجدداً بنسبة عشرة أضعاف على الأقل خلال العام 1989 وسوف يزداد على الأرجح بسرعة أكبر في العام 1990.

وقد أبرزت المشكلة موضوعاً أخلاقياً يتناول حق الفرد في الخصوصية مقابل تجميع الوقائع لإثبات حصول عمل إجرامي. وشرحت غايل تاكيري وهي محامية مساعدة في ولاية أريزونا، للّجنة الفرعية لمجلس الشيوخ بأن أحد الشواذات القانونية الذي يساعد مخرّبي الحواسيب ويحجب مدى حجم عدوى الفيروس هو قانون خصوصية الاتصالات الإلكترونية. ولم تتمكن من إخفاء انزعاجها عندما قالت بأن المؤسسات الواقعة ضحية عدوى الفيروس لا تزود المعلومات الضرورية للسلطات لتتمكن من تعقب المهاجمين وقالت للقضاة بأن «هذا القانون يحول دون حصولنا على المعلومات التي تمكننا من إلقاء القبض على هؤلاء الأشرار».

لا حلول سريعة لمشكلة الفيروس

وصف البروفسور لانس هوفمان من جامعة جورج واشنطن وهو عالم حواسيب خبير، الانقطاع الشامل للشبكات البينية التي أدت إلى توقيف أكثر من 6000 حاسوب في جميع أنحاء

الولايات المتحدة في تشرين الأول من العام 1988 على أنه بالنسبة لعالم المعالجة الإلكترونية للمعطيات مثل حادثة Three Mile Island. وقد حذر مجتمع الحواسيب ليحضّر نفسه لكارثة محتمة شبيهة بحادثة مفاعل تشرنوبيل في الاتحاد السوفياتي.

«شبكات حواسيبنا أصبحت حيوية بالنسبة إلينا مثل شبكات طرقاتنا السريعة وهواتفنا الوطنية». هذا ما قاله البروفسور هوفمان وحذر من تكاثر الفيروسات الذي قد يتطلب قانوناً ينظم حق استعمال تلك الشبكات كما الحال مع حق استعمال العربات. ولكنه حث هو والخبراء الآخرون على تجربة إجراءات بديلة أخرى قبل تقييد التبادل الحر للمعلومات منعاً من التعارض مع التشريع الأول من الدستور الأميركي المتعلق بالحرية.

وحذر جون بيكيت رئيس جمعية مصنعي معدات الأعمال والحواسيب (CBEMA). والتي تستخدم مليون ونصف مليون عامل ينتجون خمسة في المئة من الناتج القومي، مجلس الشيوخ أيضاً بأن لا يسن تشريعات ضد التقانة بل ضد المجرمين الذين يسيئون استعمالها. وقد قال للّجنة الفرعية بأن لا تتوقع من أعضاء جمعيته استنباط «حل تقني» لحل مشكلة الفيروس.

وقال بيكيت «كلما طورنا قفلاً في صناعة الحواسيب كلما قام أحدهم بتطوير مفتاح لهذا القفل».

أما الجانب البراجي لصناعة الحواسيب والذي مثله جون لاندري رئيس مجلس إدارة لجنة الفيروس للجمعية الصناعية لخدمات وبراجيات الحواسيب فلم يعط حلولاً أيضاً وقال بأنه «لا توجد معجزات».

وشدد جون لاندري على حرص صناعة الحواسيب و القطاع القانوني بأن يحدد المشرعون بدقة متناهية الفيروسات وتفريقها عن علل البراجيات وغيرها من مواربات البرمجة. واعطى كمثال قضية أعلن فيها القاضي بأن مفتاح الوصول (شيفرة توضع في البرامج لمنع اولئك الذين لم يدفعوا ثمن البرنامج من استعماله) هو فيروس من الناحية القانونية. وقال بأنه من الممكن معارضة القاضي على أساس التعريف التقني للفيروس ولكن من الناحية الأخلاقية قد يكون على صواب وذلك لأن هذه الأداة الهندسية البراجية القوية أدت إلى التوقف الكلي لبرنامج يستعمل في مختبر طبي. وهذا القرار يشير إلى أن استعمال جميع أنواع البرمجة الهدامة لحماية حقوق الملكية الثقافية للبراجيات، أوكوسيلة لجبر المستعملين على دفع فواتير الموردين أو مستشاري الحواسيب لم يعد مقبولاً.

وقال جوزف تومبكنس رئيس مجلس إدارة فريق عمل جمعية المحاماة الأميركية المختصة بجرائم الحواسيب، بأن الحظر القانوني وتطبيق القانون لا يشكلان سوى جزء من الحل لمشكلة

الفيروس كما الحال عند التعامل مع مرض اجتماعي آخر مثل توزيع المخدرات الممنوعة. واشار إلى أن هذا يشكل فرصة لتغيير القوانين المتعلقة بالدخول غير المشروع إلى أراضي الغير، وجرائم الحواسيب والأهمال الاجرامي والتزوير وما شابه ذلك وذلك كبدائل ممكنة وقوانين جديدة.

وإدخال قوانين حظر مدنية قد تساعد على توزيع حمل الملاحقة القضائية على افتراض أنه إذا استطاعت المؤسسات إزالة الأضرار التي سببها الهجوم الفيروسي فأنها تصبح أكثر تحمساً لرفع دعاوى قضائية. ولكن في الواقع من المستحيل تحديد الجهات التي تنشيء البرامج الفيروسية أو تلك المسؤولة عن انتشارها في أنظمة معينة عن قصد أو غير قصد. ومعظم الفيروسات ينشئها أفراد وفي السر. وهو عمل فردي عادةً ينفذ على شكل عمل تخريبي إلكتروني، أو مزاح شرير أو انتقام أو موقف تحدي ضد هدف معين أو ضد المجتمع ككل.

ولم يتلق قطاع الحوسبة الأميركي أية مساعدة عملية من الدوائر الحكومية مثل مكتب الاستخبارات الفدرالي أو وزارة الدفاع أو وكالة أمن الدولة رغم أن الدفاع ضد الفيروسات المحلية والغريبة هو من أساس عملهم الوطني.

وبعض الخبراء الذين تعاونوا مع مجلس الشيوخ يعتقدون بأنه من الأفضل تسليم موضوع البحث والدفاع ضد الفيروس إلى الأشخاص الذين يعرفون هذا الموضوع التقني وليس إلى الوكالات الحكومية. وقد تعالت أصوات تنتقد أولئك الأشخاص المسؤولين عن أمن الحواسيب الذين أخفقوا في التعلم من ضعف النظام UNIX في وجه عدوى الفيروس. ولو كانت تجربة الشبكات البينية مفيدة لما كان نظام وكالة الفضاء الأميركية NASA تعرّض بعد سنة تقريباً إلى نفس الحالة.

ووصف مارك روتنبرج، مدير مؤسسة محترفو الحواسيب ذوي المسؤولية الاجتماعية في مثال آخر، الخطأ الذي اقترفه فريق وزارة الدفاع الأميركية الخاص بالدفاع عن الحالات الطارئة للحواسيب. فقد نصح فريق العمل الخاص هذا المستعملين بمكافحة الفيروس ببرنامج قد يؤدي بدوره إلى نشر العدوى في أنظمتهم!

الخطوة الأولى نحو استعادة السيطرة على الحاسوب

لقد ظهر مع بداية عقد التسعينات إثباتات مزعجة تشير إلى وجود مخطط دولي ومنظم لنشر عدوى الفيروس. فقد استلم الآلاف من الاخصائيين في مجال الطب والأعمال قرصاً في البريد تشير لصيقته إلى أنه يحتوي معلومات عن مرض الإيدز. ولكن حالما يتم وضع القرص في سواقة الأقراص يبدأ باتلاف المعطيات.

وهذه العملية استوجبت استثماراً كبيراً جداً لتغطية تحضير لوائح المراسلة ونسخ الأقراص والطباعة واكلاف البريد وإنشاء مؤسسات وهمية لتغطية العملية. والأكيد أن الجهات وراء هذا المخطط كانت مصممة على الحاق الضرر بأنظمة معالجة معطيات مهمة حول العالم والإثبات هو المجهود الكبير الذي بذلته لتوزيع هذا القرص.

ويمكننا توقع أمثلة كثيرة من هذا النوع على مدى الجهد الذي يستعد الأفراد والمجموعات بذله لتخريب الحواسيب. وهذا الكتاب سوف يساعدك ويساعد مؤسستك في حال كنت مسؤولاً عن إدارة مرافق لمعالجة المعطيات على فهم هذا الخطر وتعلم طرقاً فعالة لمحاربته واستعادة سيطرتك على الحاسوب.

الفيروسات تبرز من كل حدب وصوب وتتجه نحونا من جميع الاتجاهات كما سترى في الفصول التالية. ولا يمكن اعتبار أي نظام بمنأى كامل عن الخطر وهذا يشمل البرمجة الداخلية للرقائق والتي تتحكم بأدواتك المنزلية، وأنظمة نقل الحركة الأوتوماتيكية والمكبح وحقن الوقود في سيارتك، والطيار الأوتوماتيكي ونظام حركة الطيران وغيرها من أنظمة الأمان المحوسبة لوسائل النقل الجوي، والحواسيب المستعملة في المستشفيات ومرافق الطوارىء وقوى الدفاع الجوي وغيرها من الأوجه الحيوية لمجتمعنا الحالي.

وهنالك منحى مزعج للفيروسات وهو تركيزنا على البرامجيات التجارية بحيث لا يمكن اكتشاف بعض أنواعها المتطورة. وقد يكون السبب هو انزعاج مرتكبي هذا العمل من الأرباح الطائلة التي تجنيها شركات البراجيات الكبيرة، أو قد يشعرون بأن الأفكار والمفاهيم التي يجب أن تكون ملك للعامة قد خطفتها الشركات الكبيرة واحتكرتها.

ولحسن الحظ فإن عدوى الفيروس لا تزال الاستثناء وليس القاعدة ولكن المنطق الحسابي يفرض بأن تعرضنا للخطر سوف يزداد بمعدلات متسارعة عالية إلاّ إذا قامت أغلبية مستعملي الحواسيب بأعمال وقائية. والمهم في الأمر قيام الأفراد والمؤسسات الذين تهمهم الحوسبة بتبني سياسات شاملة ومنسقة للدفاع عن أنظمتهم ضد عدوى الفيروس والقيام بأعمال فعالة في حال حصول عدوى.

وهذا الكتاب هو أداة عملية تساعد على صوغ وتطبيق هذه الإجراءات الوقائية والدفاعية. ولا تحتاج لأن تكون خبيراً في الحواسيب لمعرفة ما هو ضروري للتحكم بحاسوبك.

حقيقة فيروسية

يمكن منع 95 بالمئة من جميع حالات العدوى الفيروسي بممارسة أساليب احترازية بسيطة وآمنة عند العمل مع الحاسوب.

وفعلاً، فقد أعد هذا الكتاب على أساس عدم حاجتك إلى دراسة طريقة عمل الحاسوب وبرامجه لتتمكن من الاستفادة من هذه التقانة الرائعة. ولا يرغب معظمنا بأن يكون مبرمجاً بل تقتصر رغبتنا على جعل الحواسيب تعمل لخدمتنا مثل السيارات والثلاجات وأجهزة التلفزة التي تعمل دون أن تتوقع أن نكون خبراء في التقنيات الإلكترونية أو الهندسية.

ولسوء الحظ فإن فيروسات الحواسيب تعيد مجدداً طرح الواقع المزعج الذي يشير إلى أن الآلات قد «تعصي الأوامر» ولا تقوم بما نريده بسبب الأخطاء الناتجة عن تركيبها أو طريقة استعمالها. وقد جعلت الفيروسات من الجهاز الذي أضحى أهم جهاز في هذه المرحلة من عصر الآلة، جهازاً لا يوثق بطريقة عمله إطلاقاً. وبغض النظر عما إذا كنت تعتمد على الحاسوب لتنظيم أفكارك لتأليف قصه روائية، أو لمراقبة الإشارات الحيوية لمريض تجري عملية جراحية لقلبه، أو لتسجيل حسابات أعمالك أو لتحويل الأموال من حساب بنك إلى حساب آخر أو لتكملة الوصلة عند الاتصال هاتفياً بالمنزل، يجب أن تحذر فالحواسيب لم تعد تنفذ عملية ممكننة لا تتوقف سوى نتيجة عطل ميكانيكي أو خطأ بشري.

ولكن لا تلق اللوم بالنسبة للفيروسات على التقانة أو الآلات التي تنفذ تلك التقانة. فالحقيقة الأساسية حول فيروسات الحاسوب هي أنها مشكلة أشخاص. فالأشخاص ينشئون الفيروسات لأسباب مختلفة فهم ينشرون عدوى الفيروس إما عن قصد أو نتيجة الميزة البشرية المتمثلة بالجهل أو البراءة أو عدم الاكتراث. والأشخاص الذين يشكلون الضحايا الرئيسية لهذه الظاهرة بإمكانهم تعلم كيف يحولون خطراً حقيقياً إلى خطر محسوب ومعقول يمكن تحمله.

> **إذا لم تكن قد تعرّضت شخصياً لعدوى فيروس الحاسوب فإن الواقع الإحصائي للنمو المضطرد لمعدل حالات العدوى يشير إلى أنك سوف تلتقط هذه العدوى قريباً.**

حالما تفهم أسس إنشاء الفيروسات وانتشارها فإنك تصبح قادراً على اختيار استراتيجية دفاعية معدة خصيصاً لتتلاءم مع حاجاتك الخاصة. وقد تقرر عدم القيام بأي عمل وترك الأمر للقدر أو إلى أن أعمال الحوسبة التي تقوم بها تجعلك في فئة احتمال الخطر فيها منخفض نسبياً. ولكن قبل اتخاذ هذا القرار انتبه إلى أن الإجراءات الاحترازية التي تخفف من خطر العدوى الفيروسية ليست متطلبة وفائدتها تبرر المجهود المبذول لتطبيقها.

وإذا لم تكن قد تعرضت شخصياً لعدوى فيروس الحاسوب فإن الواقع الاحصائي للنمو المضطرد لمعدل حالات العدوى يشير إلى أنك سوف تلتقط هذه العدوى قريباً. والحجم الضخم للضغوطات الفيروسية الذاتية التناسخ المنتشرة حالياً يشير بمفرده إلى أن خطر العدوى على الأنظمة وبالأخص تلك المرتبطة عبر شبكات اتصال، سوف يتفاقم أكثر وأكثر.

إذا مارست في عملك مبادىء حوسبة أساسية وآمنة فمن غير المحتمل أن يتعرض نظامك للعدوى. وإذا استعملت برامجيات فعالة لمنع الفيروس واكتشافه فإن خطر تعرض معطياتك للتلف أو للخطر ينخفض كثيراً. وإذا نفذت الوسائل الاحترازية البسيطة المطلوبة لتسهيل التعافي بعد حصول عدوى فلن تخسر بايتاً واحداً من المعطيات خلال الوباء الفيروسي.

وفي الواقع فإنه ببذل مجهود ضئيل تنخفض فرص تعرضك للعدوى بنسبة 95 بالمئة أو أكثر، كما تزداد فرص التعافي. والوقائع التي يتضمنها هذا الكتاب يجب أن تزودك بكل ما تريد معرفته عن فيروسات الحواسيب وبنفس الوقت توفر لك بضعة ساعات من القراءة الممتعة.

2 كيف يجعل الفيروس الحاسوب مريضاً

كيف يدخل الفيروس في الحاسوب ويحول حالته الطبيعية الصحية إلى حالة مرضية إلكترونية؟ وتتضح هذه العملية أكثر عند مقارنتها بالطريقة التي يمرض بها الجسم البشري عندما يغزوه فيروس مُعْدي.

تستعمل البراجيات للتفاعل مع الحاسوب. وبدون البراجيات يصبح الحاسوب مجرد آلة عديمة الفائدة. والبراجيات هي الوسط الذي ننقل بواسطته التعليمات إلى الآلة (الحاسوب) وكذلك آلية التحكم التي تمكن الآلة من تنفيذ تلك التعليمات تنفيذاً صحيحاً وهي المعادل الحاسوبي للعقل البشري والنظام العصبي المركزي. وبسبب تعقيد الحاسوب كجهاز قادر على القيام بعدة أعمال مختلفة فإن التعليمات المستعملة لجعله يعمل بطريقة معينة، معقدة أيضاً.

ولهذا السبب ولجعل الحوسبة أسهل واسرع فإننا نستعمل نوعين من البرامج يكتبها الخبراء. الأول هو **نظام التشغيل** (operating system)، وهو البرنامج الرئيسي الذي يتحكم بجميع وظائف الحاسوب الأساسية. مثلاً فهو يدير طريقة عمل سواقات الأقراص وانطلاقاً من هذا السبب فإن اللفظة الأوائلية DOS تشير إلى أكثر هذه البرامج شعبية وهو اختصار للجملة Disk Operating System أو نظام تشغيل الأقراص. وحواسيب الماكنتوش (Macs) والأميغا (Amiga) والحواسيب المتوسطة (minicomputers) والحواسيب الأيوانية (mainframes) تملك جميعها برامج لأنظمة التشغيل. وقد تكون أنظمة التشغيل متميزة بتصميمها البنيوي (architecture)، فالمجموعة System و Toolbox لحواسيب الماكنتوش تختلف جذرياً عن النظام DOS ولكنها تنفذ نفس الوظائف. وهذا يعني بأن جميع أنظمة التشغيل عرضة لفيروسات الحواسيب والتي مثل الفيروسات البيولوجية «خاصة بالنوع الاحيائي». ومثلما تتعرض الحيوانات إلى حمى حيوانية فإنها لا تتأثر بالانفلونزا البشرية. تلتقط حواسيب الماكنتوش الفيروس MacMag بينما تلتقط الحواسيب الشخصية صنع IBM أو الحواسيب المتوافقة معها فيروس Jerusalem.

وهنالك بضعة أنواع من برامج أنظمة التشغيل ولكن هنالك العديد من الأمثلة عن النوع الثاني من البراجيات التي نستعملها وهي **البرامج التطبيقية** (application programs).

وهذه البرامج تعمل بالتعاون مع نظام التشغيل لتنفيذ مهام محددة مثل معالجة الكلمات أو إنشاء الصفحات المجدولة أو الألعاب أو توليد تصميمات تخطيطية.

وإذا كنت لا تعرف كيف تعمل الحواسيب فيمكنك مقارنة إجراء استنهاض (boot-up) الحاسوب بما تفعله عند النهوض صباحاً. جسمك هو العتاد في نظام الحاسوب، وخلال نومك يلعب دماغك والجهاز العصبي دور برامجيات نظام التشغيل للحاسوب عاملين على توقيت ضربات القلب بانتظام للمحافظة على سريان الدم عبر الشرايين والأوردة ومراقبة التنفس وغيرها من الوظائف الحيوية والسيطرة عليها.

وعندما تنشّط جسمك من حالة الرقود هذه فإنك تصدر إليه تعليمات ليقوم بمهام معينة كالقيام من الفراش والاستحمام وصنع القهوة وقيادة السيارة للوصول إلى مركز العمل. وهذه الأوامر الطوعية التي «تلقمها» في دماغك تعادل البرامج التطبيقية للحاسوب التي تلقمها في الحاسوب.

عندما يكون جسمك كامل الصحة فكل شيء يكون منضبطاً ومتوقعاً. وتعطي جسمك تعليمات تجعله يقوم بمهمة معينة فيقوم دماغك وجهازك العصبي بتنسيق عمل أذرعك وارجلك ويديك وعيونك للقيام بتلك المهمة. أما إذا التقط جسمك عدوى فإن «نظام التشغيل» و«البرامج التطبيقية» قد لا تعمل بشكل جيد، فيلاقي الدماغ صعوبة بالتحكم بالوظائف الأساسية. قد تحاول جعل جسمك يؤدي مهمات معينة مثل الركض مثلاً ولكن رأسك واطرافك توجعك وجسمك وهن. لقد منعت العدوى جسمك من إتمام المهام المطلوبة.

يؤثر فيروس الحاسوب بنفس الطريقة على الحاسوب. وهو يستطيع إلحاق الضرر بقدرة نظام التشغيل على التحكم بالوظائف الأساسية وعند تشغيل البرامج التطبيقية فإنه يتجاوز نشاطاتها أيضاً.

كيف يدخل الفيروس في النظام

رغم أن الفيروس هو برنامج برامجي بشيفرة تقوم بغلق وفتح الدوائر الكهربائية داخل الحاسوب مثل نظام التشغيل والبرامج التطبيقية فإنه يتميز بفارق مهم. البرامج العادية هي وسائل تساعدك على العمل وتشتريها على أساس أن كل من ساهم في تصميمها وتوزيعها هو حليفك وله نفس هدفك وهو مساعدتك في مهامك الحاسوبية.

أما أولئك الذين ينشئون الفيروسات فيكتبون البرامج بدوافع مختلفة كلياً. وبسبب رغبتهم بتسبيب المشاكل فإنهم يكتبون برامج تضر ولا تساعد. وقد ينشئون برامج تحمل

رسائل غير مجدية على شكل بريد إلكتروني تافه أو نوع من أنواع الدعايات الرخيصة. وبما أنك لا تحتاج إلى مثل هذا النوع من البرامجيات ولن تقوم بالتأكيد بشرائها أو حتى قبولها كهدية فإن صانعي هذه البرامج يجعلونها جذابة أو ذكية بما يكفي لجعلك تسمح بدخولها إلى نظامك.

واحدى الطرق هي تمويهها بحيث تبدو كبرامجيات مصممة لمساعدتك مثل حصان طروادة (Trojan Horse). وقد تبدو البرامج الضارة وكأنها برامج مثيرة للاهتمام ومفيدة مثل لعبة حاسوبية أو برنامج تطبيقي موفر للوقت وذلك للاستئثار بانتباهك. وتوضع مثل هذه البرامج على لوح الإعلان حيث يقوم المستعملون بتلقيمها في الحاسوب معتقدين بأنهم يستلمون برنامجاً مسلياً أو مفيداً.

حقيقة فيروسية

يكون السبب وراء التصرف الغريب للحاسوب في معظم الأحيان نتيجة علة في البرامجيات وليس من الفيروس. راجع الملف README الذي يرفق مع البرامج التطبيقية واتصل بوكيلك لمعرفة عما إذا كان ما تعانيه هو علة ولا علاقة للفيروس به.

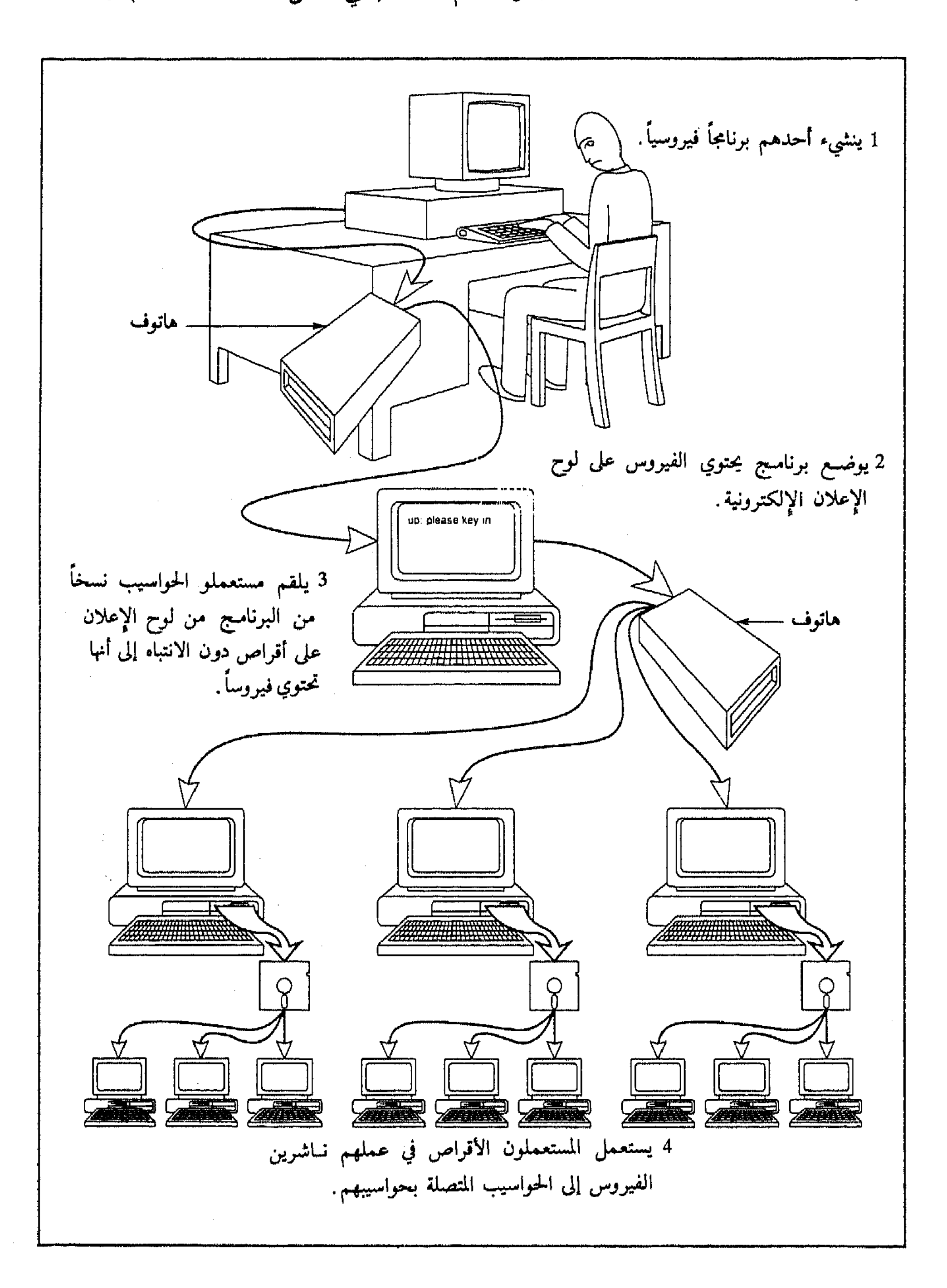
وهذه الطريقة ليست فعالة جداً إلّا إذا كان البرنامج الضار هو فيروس حاسوبي. ويقوم الفيروس نيابة عن صانعه بمهمة نشر البرنامج الفتاك إلى عدة أهداف وذلك بنسخ نفسه وإرسال النسخ إلى الخارج للدخول في أنظمة أخرى. وبهذه الطريقة فإن العمل الضار أو الرسالة الضارة سوف تنتشر بسرعة وبكثرة.

يكفي شخص واحد لتلقيم الفيروس من لوح الإعلان لكي تنطلق عدوى الفيروس إلى عدة حواسيب. وحالما يصبح داخل نظام المستعمل الذي لقمه فإنه يستطيع تلويث الملفات الموجودة في القرص الصلب والأقراص المرنة. وبعد ذلك وعندما تتفاعل الضحية الأولى مع الحواسيب الأخرى على شبكة الحواسيب، أو تعطي قرصاً ملوثاً إلى صديق، أو تلقمه في نظام عامل فقد ينتشر الفيروس ويتسنى له التناسخ والحاق الأذى.

ومع انتشار وباء الفيروس نلاحظ وجود الآلاف من أنظمة الحواسيب التي تشغل ثلاثة أنواع من البرامج هي برامج أنظمة التشغيل العادية، والبرامج التطبيقية التي يركبها ويتحكم بها المستعمل، وبرنامج فيروسي على شكل دخيل متخفي وغير مرغوب به. وحالما يصبح داخل النظام يستطيع الدخيل الفيروسي التصرف بعدة طرق وذلك إما بكشف وجوده مباشرة أو البقاء متخفياً محدثاً الضرر ومتناسخاً.

ويفرض المنطق تصميم الفيروسات بحيث تدخل الأنظمة عبر الملفات التي تصادفها كثيراً عند وصولها. ولهذا فإن الملفات التي تحمل اللواحق COM . و EXE . و SYS . والتي

تشكل جزءاً من كل نظام DOS هي الأهداف الأولى لهذا الفيروس. ولدى أنظمة التشغيل الأخرى نقاط ضعف مماثلة. ملفات الأوامر للنظام DOS (التي تحمل اللاحقة COM .) والملفات



EXE . هي برامج قابلة للتنفيذ تمكّن النظام DOS من أداء وظائف مهمة. تعرّف اللاحقة SYS . الملفات النظامية التي تشكل أيضاً جزءاً أساسياً من براجيات التحكم للنظام DOS. وهنالك أيضاً ملفات نظامية لا تسرد في دليل الملفات ولذا تشكل مكاناً جيداً لاختباء الفيروسات.

ويميل العديد من الملفات القابلة للتنفيذ (أي أن النظام يستطيع تشغيلها) إلى التحفيز خلال إجراء الاستنهاض الأولى عند وصل الحاسوب بالطاقة. ولهذا السبب فإن العديد من الفيروسات مصممة بحيث تلصق نفسها بهذه الملفات لأنها موجودة دائماً مع النظام DOS وهي تؤدي وظائف قوية وحيوية وهي عادةً الملفات الأولى التي يجري تشغيلها عند بدء اشتغال الحاسوب.

ويستطيع العديد من البرامج التطبيقية إنشاء أوتعديل الملفات CONFIG.SYS و AUTOEXEC.BAT الموجودة أصلاً. وقد صمم النظام DOS بحيث يبحث عن تلك الملفات في المراحل الأولى من عملية الاستنهاض وذلك للحصول على التعليمات المتعلقة بطريقة تشكيل النظام وعما إذا كان من الواجب تشغيل ملف معين قام المستعمل أو البرنامج التطبيقي بتحديده سابقاً. ولهذا السبب فإن الفيروس يبدأ قبل معظم برامج إكتشاف الفيروسات منهياً عمله في جزء من الثانية خلال استنهاض الحاسوب وقبل أن يبدأ البرنامج المضاد للفيروس عمله.

كيف يتحكم الفيروس بالنظام

أحد أكثر أوجه الوباء الفيروسي إزعاجاً هو أن مستعملي الحواسيب العاديين بدأوا يفقدون سيطرتهم على محيط عمل حواسيبهم. الأوامر التي تصدرها كمستعمل للحاسوب إلى نظام التشغيل والبرامج التطبيقية قد يتم تجاوزها من قبل الفيروس إذا ما كان قد صمم لهذا الغرض. واستلام زمام الأمور هذا يمكن تحقيقه بعدة طرق حالما يصبح الفيروس داخل النظام وحسب طريقة برمجته. ومجدداً لا يستطيع المستعمل أونظام التشغيل أو البرامج التطبيقية التحكم بهذا الوضع وذلك لأن الفيروس غير مصمم ليعمل وفق مبادىء العمل المتبعة عادةً. وهو قد يعمل مثل طفل عنيد يقوم بعمل عكس ما تريد منه عمله. وهو قد يعيث الفوضى في ملفاتك تالفاً إياها أو مغيراً لها كيفما يريد

والكلمة الأساسية وراء فهم طريقة عمل الفيروسات هي التحكم. توقف الفيروسات الملوثة للملفات EXE . و COM . نشاط الحوسبة العادي في أول فرصة تسنح لها باستلام سلطة التحكم على النظام لتقوم بعد ذلك بنسخ نفسها ولصقها بملفات EXE . و COM . أخرى.

يعيث الفيروس الفوضى في ملفاتك تالفاً إياها أو مغيّراً لها كيفما يريد.

وقد يلتصق الفيروس بالملفات من الخارج مثلما تضع لصيقة على الجهة الخارجية لحافظة الملفات الورقية العادية. وقد يجد فراغاً داخلياً يتسع لشيفرة الفيروس ضمن شيفرة البرنامج الذي انتقاه كمضيف. وهذا مماثل لإخفاء قصاصات من الورق ما بين صفحات من الورق توضع عادة حافظة الملفات العادية.

وعملية مقاطعة الفيروس لنشاط الحوسبة العادي والتي يتبعها استلام الفيروس لسلطة التحكم بالنظام من أجل التناسخ وتنفيذ مهام أخرى في برنامجها ومن ثم إعادة سلطة التحكم إلى نظام التشغيل والبرامج التطبيقية، قد تحصل بسرعة كبيرة بحيث لا ينتبه المستعمل إلى شيء.

وتبقى بعض الفيروسات الملوثة للملفات COM . و EXE . مقيمة في ذاكرة النظام بحيث تعمل على تلويث كل برنامج يجري تنفيذه. وهي تستطيع تعديل قطاع الاستنهاض للقرص لجعله محيط عمل أكثر ملاءمة لتناسخ الفيروس ولنشاطاته الأخرى. كما تستطيع أيضاً تغيير البرامج التطبيقية بحيث تكون أكثر ملاءمة لاحتياجات الفيروس.

قد يبحث الفيروس عن ملف نظامي محجوب أصلاً، أو قد يغير أحد الملفات إلى ملف محجوب بحيث لا يظهر في سرد دليل الملفات.

وتختبأ بعض الفيروسات في البراجيات التي تتحكم بساعة التوقيت الداخلية للنظام (الميقت أو clock). وغالباً ما يكون العمل الأول للفيروس هو التدقيق في وقت وتاريخ النظام ليرى عما إذا كانا يتوافقان مع وقت التحفيز المبرمج للفيروس. وأحد الأعمال الأولى التي يقوم بها الفيروس هو تحديد عما إذا كان هنالك من ملفات أو أقراص في النظام لتقوم بتلويثها. وإذا لم يجدها فقد يعيد التحكم إلى نظام التشغيل أو البرنامج التطبيقي وينتقل إلى حالة من السكون متربصاً بالنظام إلى حين بروز وضع يساعده على التفشي.

والكثير من حالات انتشار العدوى عبر شبكات الحواسيب وداخل المؤسسات يمنع منعها بالحد من تبادل البرامج القابلة للتنفيذ. مثلاً، عند تشارك عدة مستعملين في استخدام طابعة لا يزرية فإن الأقراص المستعملة لطباعة المستندات يجب أن لا يحتوي سوى معطيات.

وقد تعمل الفيروسات بنفس الوقت مع نظام التشغيل أو البرامج التطبيقية التي لوثتها منفذة مهماتها إما علناً أو بشكل خفي. وهنالك فيروسات أسمية ملوثة للبرامج التطبيقية مبرمجة للسيطرة على البرامج التطبيقية لحظة تشغيلها وتغييرها بطريقة ما ومن ثم إعادة التحكم إلى

البرنامج التطبيقي. وهذه الفيروسات قد تختبىء في البرنامج التطبيقي وتستلم بعضاً من وظائفها أو تلصق نفسها عادة بنهاية أو بداية الملفات. والبرامج الملوثة تصبح بدورها فيروسات ناشرة العدوى والبرمجة أو الرسالة المضرة التي يحملها الفيروس.

وتتحكم بعض الفيروسات بجداول تخصيص الملفات FAT التي تنظم طريقة التخزين على القرص، أو تلحق الضرر بقدرة الجداول FAT على معرفة الموضع الفعلي للمعطيات على القرص. وما يقوم به الفيروس فعلياً هو إعادة رسم خريطة القرص أو اتلافها بحيث لا يستطيع نظام التشغيل إيجاد طريقة إلى أي موقع على القرص حيث تحفظ المعطيات.

والفيروسات التي ترسل نسخاً عن نفسها إلى منطقة الذاكرة العشوائية الوصول (RAM) وهي منطقة عمل الحاسوب الرئيسية تستطيع البقاء مختبئة وجاهزة للانقضاض على أي مضيف متقبل يمر مثل قرص مرن غير ملوث يجري وضعه في سواقات الأقراص المرنة. قد تأخذ قرصاً مرناً نظيفاً وجديداً من غلافه الورقي وتقوم بنسقه لأول مرة في السواقة A ليصبح مباشرة وسطاً يستضيف الفيروس الجاثم في الذاكرة RAM، أو في القرص المرن في السواقة B أو في القرص الصلب. والفيروسات مثل الذباب المنتظر في الأعشاب جاهز للانقضاض على أول كلب مار.

حقيقة فيروسية

البرامج المقرصنة (المنسوخة بلا إذن) هي أحد المصادر الرئيسية للفيروسات. لا تقم أبداً بتشغيل برنامج امتلاكي غير موجود ضمن رزمته المغلقة الأصلية دون اختباره أولاً. واحذر بشكل خاص وكلاء التوزيع الذين يعرضون عليك تلقيم القرص الصلب في حاسوبك ببرامجيات «مجانية». فهذه البرامجيات هي برامجيات مقرصنة على الأرجح أو برامجيات عامة وقد تكون ملوثة.

وكما سنرى في الفصول اللاحقة فحالما يلوث الفيروس أحد الأنظمة فإنه قد يمنع ذلك النظام من العمل بفعاليته العادية أو قد يولد عوارض أكثر حدة من المرض الإلكتروني أو يعيق الوظائف بحيث لا يعد بمقدور النظام تنفيذ مهماته. وتقوم بعض الفيروسات فعلياً بقتل النظام وذلك بإتلاف الملفات التي يحتويها. وكما الحال مع بعض الفيروسات البيولوجية فقد تحتاج الفيروسات إلى وقت طويل قبل استفحالها بحيث قبل ظهور علامات واضحة عن وجود مشكلة يكون التلوث قد تركز جيداً وانتشر كثيراً وبالتالي أصبحت إزالته أكثر صعوبة.

ومدى الضرر الذي يلحقه الفيروس لا يعتمد دائماً على تعقيده أو حجمه أو تطوره. فالفيروس البسيط الذي يقوم بسرعة بتعديل الجدول FAT وينفذ أمر نسق القرص الصلب أو يتلاعب ببضعة بايتات من المعطيات في الدليل الجذري للحاسوب الشخصي أو في الملف Desktop لحاسوب الماكنتوش قد يكون تأثيره فتاك على نشاطات معالجة الكلمات. وحتى ولو كان

الضرر الفعلي ضئيل فإن العواقب قد تكون وخيمة. فهنالك فيروسات يقتصر عملها على تغيير بايت من المعطيات هنا وهناك بطريقة عشوائية وذكية لا يلاحظها أحد لفترة طويلة. وقد لا يكون الضرر كبيراً إذا ما كانت نتيجته مجرد أخطاء طباعية في مستند معالجة الكلمات. ولكن العواقب قد تكون أكثر سوءاً إذا ما تم تعديل الأرقام في معطيات المحاسبة أو في معادلة لتركيب أحد الأدوية.

> يشبه العديد من حالات الأداء السيىء الروتينية للحاسوب العوارض الفيروسية. ولا يجب الجزع عندما تكون المشكلة مجرد علة في البرنامج أو سوء أداء عتادي.

قد يتلوث حاسوبك دون وجود عوارض مرض. وبكلمات أخرى قد يكون حاسوبك ناقل للفيروس. ونتوقع حصول ذلك كثيراً بسبب تزايد إنشاء الفيروس لأغراض خاصة وتوجيهها إلى أهداف معينة مثل أنظمة الحكومة والمؤسسات. وهذه الفيروسات تجد طريقها إلى الهدف أما بالمرور عبر أنظمة أخرى أو بالهروب إلى عالم الحوسبة العام. وإذا كانت مبرمجة بحيث تمنع نفسها من العمل أو إلحاق الضرر إلا عند وصولها إلى هدف معين فإن هذه الفيروسات لن تلحق الضرر غير المقصود بالأنظمة التي تمر عبرها. ولكن العديد من هذه الفيروسات المختصة بهدف معين بإمكانها تعطيل حواسيب غير تلك المستهدفة وذلك باستعمالها لإجراء أعمال التناسخ الجنونية. وإذا كان الفيروس نفسه يحتوي على علة في برمجته فقد يصبح كصاروخ غير موجه فقدت السيطرة عليه.

من السهل أن يصبح المرء متوسوساً بخصوص معالجة المعطيات. والعديد من حالات سوء الأداء الروتينية للحواسيب تشبه العوارض الفيروسية. ولا يجب الجزع عندما تكون المشكلة مجرد علة في البرنامج أو سوء إداء عتادي لن ينتشر أو يضر بالمعطيات أو يتطلب مساعدة الخبراء باكلاف باهظة. وسوف يشرح الفصل الخامس هذه الأسباب الأخرى للعوارض الفيروسية بالتفصيل.

ورغم أهمية اعتماد أساليب حوسبة آمنة لتخفيض مخاطر حصول عدوى فيروسية إلى أدنى حد فلا حاجة إلى أن يصبح المرء مريض الشك إلى حد يفقد فيها متعة وفوائد الحوسبة. فالسماح لخطر الفيروس بأن يحصر استعمال شبكة الحواسيب كثيراً مثلاً قد يلحق ضرراً أكبر من الدخول في مخاطرة محتسبة بعد اعتماد إجراءات وقائية أساسية.

والأهم أن تتذكر بأن تلوثات الحاسوب سوف تخضع في النهاية إلى سيطرتنا أكثر من الفيروسات البيولوجية التي تتفشى في أجسامنا. ولا نملك حتى الآن حلاً تقنياً سريعاً وناجعاً، أو معجزات أو حبوب عجائبية تشفي فوراً، ولكننا نملك ترسانة أسلحة شاملة من وسائل الدفاع

والعلاج. ولا يكون تلوث الحاسوب فتاك بالضرورة في نظام تم فيه إتخاذ إجراءات احترازية مناسبة بالنسبة لسجلاته الحيوية وتم تطبيق إجراءات الاستعادة والتعافي المفصلة في هذا الكتاب. وتستطيع دائماً تقريباً إعادة إنعاش الحاسوب وجعل قلبه ينبض بانتظام عن جديد بواسطة بضعة أوامر أساسية فقط!.

3

الأسئلة العشرون الأكثر تداولاً بخصوص فيروس الحاسوب

سألني أحد الصحافيين خلال الهلع الذي ساد أوساط الإعلام حول فيروس يوم كولومبس «هل من الصحيح بأنني استطيع شراء جهاز يوضع في الثقب الموجود وسط الأقراص المرنة لمنعها من التلوث بالفيروسات؟ لقد سمعت بأن هذه الوسائل الواقية فعالة».

وهذا السؤال هو واحد من الأسئلة التي يسألها أولئك الذين معرفتهم بالحواسيب ضئيلة جداً. وفي الواقع لا يمكن اعتبار أي سؤال حول الفيروسات وطريقة مكافحتها سؤالاً ساذجاً. فقد أصبحت فيروسات الحواسيب ظاهرة تتخطى تجاربنا السابقة مع العمليات الميكانيكية والإلكترونية بحيث يجب الإجابة على أكثر الأسئلة بداهة.

لقد تخطت تقانة الحواسيب نطاق الخبراء لتصبح أداة يستطيع الجميع استعمالها دون مهارات خاصة. ونعيش حالياً في عصر التقانة العالية ولكن معظمنا يجهل كيف تعمل أدواتنا والعابنا العالية التقانة. هنالك أجهزة فيديو في أكثر من 80 بالمئة من منازلنا ولكن معظمنا لا يعرف كيف يشغل جميع أزرار التحكم على تلك الآلات. الرئيس الأميركي رونالد ريغان الذي كان يتحكم بقدر من القدرة التقنية الهائلة لم يسبق لإنسان قبله أن تحكم بها اعترف بأنه يجد صعوبة في تشغيل جهاز الفيديو في منزله ولا يستطيع إطلاقاً توقيفه!.

ويتجنب مستعملو الحواسيب واولئك المسؤولون عن نشاطات معالجة المعطيات طرح أسئلة أساسية خوفاً من اظهار جهلهم المخجل. وهذا يشكل مشكلة اتصال إضافية يجب أن ينتبه المدراء إليها عند محاولتهم تثقيف مستعملي الحواسيب بخصوص الفيروسات والخطر الذي قد تلحقه بالسجلات الحيوية وبعمل المشاريع التجارية. وقد يكون من المضر في أيامنا هذه بالنسبة للمستقبل المهني للموظف اظهار جهله بشؤون الحوسبة وذلك لأنها أصبحت موضوعاً يتوقع أو يفترض منا أن نلم به. أتذكر بأنني عوملت بإزدراء من قبل زملائي الإداريين لأنني لم أعرف كيف استعمل البرنامج لوتس 3-2-1 الذي يعتبره البعض أداة أساسية للارتقاء في السلم الإداري.

ولذا نميل إلى الإدعاء بأننا نعرف أكثر مما نعرفه بالحقيقة عن الحواسيب وهنا يكمن الخطر الحقيقي على أنظمة الشركات لأن الجهل المتستر قد يلحق ضرراً كبيراً. ولقد استطاع وباء الفيروس أن يجمع قوته ويتفشى في العديد من الشركات بسبب بطء العديد من خبراء الحواسيب والأمن في فهم ماهية الفيروسات ولماذا تنشىء والأخطار التي تسببها.

وأحد العوائق الكبيرة في أواخر الثمانينات للتحرك ضد خطر انتشار الفيروسات هو إقناع الخبراء بأن يعترفوا بجهلهم حول الوقائع الأساسية. والكثيرون لم يظهروا العقل المنفتح الذي أظهره مهندس برمجة قديم يملك خبرة تزيد عن عقدين من الزمن والذي اقترب مني بعد إلقائي محاضرة قصيرة عن فيروسات الحواسيب في لونغ بيتش في الولايات المتحدة. وقد تألف الحضور في معظمه من مستعملين عاديين للحواسيب ولذا اقتصرت محاضرتي على المواضيع الأساسية والبسيطة. واخبرني ذلك المبرمج بعد ذلك بأنها المرة الأولى التي استطاع فيها فعلاً فهم معنى الفيروسات وعرف مدى خطرها. وما اتمناه هو مشاهدة المزيد من الخبراء يعترفون بأنهم لا يعرفون كل شيء وأن خبرتهم نفسها قد أعاقت قوة إدراكهم.

وفيما يلي أجوبة على بعض الأسئلة الأساسية التي تسأل كثيراً حول فيروسات الحواسيب. وهي غير تقنية في مضمونها لأنك لا تحتاج سوى إلى معرفة تقنية قليلة جداً في الحوسبة لتفهم ماهية الفيروسات وما تستطيع فعله وكيف تدافع عن نظامك ضد معظمها. وفي الواقع فإن فيروسات الحواسيب ليست بمشكلة تقنية بل مسألة بشرية والتي لن تحل سوى بالجهود المشتركة للقدرات التقنية والبشرية مع جرعة كبيرة من الحس المنطقي.

السؤال رقم 1: ما هو فيروس الحواسيب؟

فيروس الحواسيب هو برنامج براجي قادر على التوالد أو التناسخ. وهو قد لا يضر بالمعطيات أو بالبرامج الأخرى. ولا يستطيع الفيروس القيام بعمل غير مكتوب في برنامجه. وهو خلق فكري من مبرمج حواسيب بشري مثل برنامج معالجة الكلمات أو برنامج الصفحات المجدولة أو لعبة غزاة الفضاء. وهنالك أنواع أخرى من البرامج المضرة مثل الديدان واحصنة طروادة التي تسمى بالفيروسات في الأوساط الإعلامية. وغالباً ما يختبىء الفيروس في حصان طروادة الذي هو برنامج ضار متنكر كبرنامج بريء.

السؤال رقم 2: ما هو الدافع وراء إنشاء فيروس الحواسيب؟

إن كتابة برنامج يصبح مخلوقاً حياً وينتشر ويتوالد وينفذ مهمات تحددها له هو تحدي فكري رائع. ولكي تواصل تقانة الحواسيب تطورها نحتاج إلى أشخاص خلاقين ومبدعين يقومون

بتجربة قدرات هذه التقانة والتعمق فيها. وانشاء برامج ذاتية التناسخ هو جزء مهم من عملية التطور خاصة إذا كنا نريد الاستفادة من القدرة الكاملة للحوسبة للقيام بمهام أكثر تحدياً. ولهذا السبب فإن العديد من الفيروسات يصنعها باحثون أو علماء تجارب مسؤولون ولكن بعضاً منها يتسرب أحياناً وبدون قصد إلى محيط الحوسبة العام. (راجع السؤال رقم 4 بخصوص الفيروسات غير الضارة).

وتصنع بعض الفيروسات كدعابات تؤدي إلى متاعب غير مقصودة. وهذه الفيروسات قد تسبب أذى كبير إذا كان برنامجها يحتوي عللاً يجعلها تتصرف بطريقة مؤذية خاصة إذا كان الفيروس ينشر عدواه دون تمييز.

ولقد وفرت الفيروسات سلاحاً لبعض أفراد المجتمع الذين يريدون الأذى للآخرين لأسباب مختلفة. وبعض هؤلاء الأشخاص هم مخربون شريرون هدفهم التخريب، والبعض الآخر له مواقف سياسية وهنالك أيضاً قسماً يريد الإضرار بالحكومة أو بالمؤسسات أو بالشركات التي يعتقد بأنها أساءت إليه.

بسبب إزدياد حجم المبرمجين فإن هنالك عدد كبير من المخربين ومرضاء العقول والأشخاص الشاذين عن المنحى العام للمجتمع الذين يعيشون فيه والذين يملكون المهارات الضرورية للتعبير عن مشاعرهم بنشر الفيروسات.

وهنالك ظاهرة التقليد التي يجب أخذها بعين الاعتبار فإذا قام أحدهم مثلاً بوضع السم في دواء امتلاكي فإن ذلك قد يؤدي إلى جعل غيره يقلده. ولكن خلافاً للعبث بالأدوية فإنك لا تستطيع منع انتشار النشاط الفيروسي المقلّد بوضع أختام ضد العبث على رزمة البراجيات. ويتنامى إنشاء الفيروسات بالذهاب إلى أبعد من نشاط التقليد البسيط إلى الإيحاء لأحدهم بأن ينشىء فيروساً أفضل. الفيروس Hypercard الذي ظهر العام ١٩٨٨ وهو الفيروس الأول المكتوب بلغة HyperTalk بدا وكأنه من وحي الفيروس MacMag والإثنان كانا يحملان رسائل سلام ومحبة ولم يظهرا أية نية في إلحاق الأذى المتعمد ولكن الإثنان قد تعرضا منذ ذلك الوقت إلى التعديل والتحسين بحيث أصبحا فيروسات مختلفة وكثيرة الضرر.

والمثير للاهتمام بشكل خاص هو احتمال كون إنشاء الفيروسات تعبير جديد عن شعور العداء الذي يشعر به بعض مهووسي الحواسيب ضد الطريقة التي تستعمل فيها الحواسيب في الشركات الكبيرة والوكالات الحكومية وغيرها من رموز المجتمع. والحوسبة هو شغف يسيطر على حياة العديد من المتحمسين. وبالنسبة للبعض فإن ذلك الشغف قد يتحول إلى تصرف مهووس خالقاً دوافع غير منطقية للانتقام من أولئك الذين يعتقد بأنهم يسيئون إلى «طهارة» مفاهيم الحوسبة.

الغيرة والشعور بالنقص قد يلعبان دوراً أيضاً في قولبة مشاعر مهووس الحاسوب. والمهووس الخارج عن مجتمعه الذي يواجه صعوبة في التعامل مع الناس والعالم الحقيقي يشعر بأن واجبه حماية محيط عمل الحوسبة الذي يرتاح إليه، من تحكم الأفراد والمجموعات الذين يبغضهم. وبتعطيل الأنظمة واتلاف المعطيات يقول بأنه يتمتع بسلطة معينة وله قوة ملموسة في مجال يعتبره ملكاً خاصاً.

السؤال رقم 3: لماذا تنتشر الفيروسات حالياً بسرعة؟ هل نواجه وباءاً لا نستطيع السيطرة عليه؟

كما شاهدنا فإن عدد الأشخاص الذين يصنعون الفيروسات يزداد وبنفس الوقت هنالك نمو مضطرد في عدد الفيروسات الموجود في محيط الحوسبة والتي تتناسخ تلقائياً أو يجري نشرها عمداً. وأي شخص يملك حاسوباً متصلاً بحاسوب آخر بواسطة هاتف أو عبر شبكة حواسيب، أو يتبادل الأقراص مع شخص آخر أو ينقل الأقراص من نظام إلى آخر يقوم عن قصد أو غير قصد بنشر عدوى الفيروس.

والقسم الأكبر من انتشار العدوى هو من الأنظمة الملوثة التي لم تظهر عليها عوارض المرض. وتبحث هذه الفيروسات عن ملفات أخرى وسواقات الأقراص لتلويثها، وحتى عن عناوين أشخاص وانظمة أخرى تستطيع زيارتها بعد ذلك منتقلة عبر التوصيلات. وهي تواصل التناسخ وإيجاد ضحايا جدد في الخفاء بحيث يكون انتشار العدوى أكبر مما يبدو فعلياً.

وفيروس الحواسيب الذي يدخل في شبكة حواسيب يستطيع التوالد والانتشار بشكل أسرع من أكثر الأجسام الحية خصباً. مثلاً البكتيريا Escherichia coli التي تنمو في أمعائنا تستطيع الإنقسام إلى نصفين متشابهين مرة واحدة كل 15 دقيقة ولكنها بطيئة بالمقارنة مع فيروس الحاسوب الذي يستطيع التناسخ عدة مرات في أقل من ثانية واحدة.

حقيقة فيروسية

إذا شككت بأن أحد البرامج الجديدة قد يكون ملوثاً ولكنك قررت رغم ذلك تشغيله ولا تملك برنامج مضاد للفيروس، قم أولاً بفتحه كملف معطيات قرائي في معالج كلمات. عاينه لترى عما إذا كان هنالك رسائل غير اعتيادية أو بذيئة ضمن تعليمات البرنامج. وهذه الرسائل هي إحدى مزايا العديد من الفيروسات. ولكن إحذر! فهذا العمل وحده قد يطلق الفيروس أيضاً.

إن معدل انتشار الفيروس محصور بفرص حصول عدوى جديدة. ولحسن الحظ فإن هذه الفرص تكون مقيدة بطريقة أو بأخرى، فعالم الحواسيب ليس بعالم مثالي بالنسبة لفيروسات

الحواسيب ولكن فرصها في التناسخ والحاق الضرر سوف يزداد كلما إزداد عدد أنظمة الحواسيب المستعملة ووصلها عبر شبكات حواسيب مع بعضها البعض وزيادة توافقيتها على تبادل شيفرة البرمجة. واحد نتائج هذه التوافقية المتزايدة ما بين أنظمة التشغيل قد يكون انتشار أنواع جديدة من الفيروسات من الأنظمة العاملة بالنظام DOS إلى أنظمة الماكنتوش والآبل والاميغا والأتاري واليونيكس وغيرها من محيطات الحوسبة. وتستطيع هذه الفيروسات في الوقت الحاضر أيضاً تلويث أنظمة مختلفة عن طريق تحولها إلى ضغوطات فرعية تنتشر في محيطات أنظمة تشغيل أخرى.

واحدى الإمكانيات المزعجة بشكل خاص هو تطوير فيروسات حاسوبية بإمكانها الطفور (mutate) كما الحال مع بعض الفيروسات الطبيعية والبكتيريا. وعندما تجد هذه «الفيروسات الخارقة» بأن قدرتها على التناسخ والعيش قد كبتت فإنها تتأقلم وتتغير لتتلاءم مع محيطها العدائي. وهنالك الآن برامج فيروسية بإمكانها الانتشار داخل برامج معينة مضادة للفيروس ومصممة لمهاجمتها. وهذا مماثل لبعض أنواع الحشرات التي لا تصبح منيعة ضد مضادات الحشرات فقط بل تستطيع النمو عليها.

السؤال رقم 4: لماذا تصبح الفيروسات غير الضارة المصممة لأغراض الأبحاث أو التجارب فيروسات ضارة؟

المهمة الأولى والأساسية التي يبرمج الفيروس لتنفيذها هي التناسخ. وهذه هي طبيعة هذا النوع من البرامج ويجب على صانع هذا البرنامج القيام بعمل خاص ومقصود لكبت قدرة التناسخ هذه.

وحتى لو قام الصانع بوضع ضوابط للحد من معدل التوالد فإن هذه الضوابط قد تخفق. وقد حصل هذا الأمر عندما أرسل طالب ألماني إلى أصدقاءه بطاقة عيد ميلاد إلكترونية أدت إلى تلويث الشبكة الدولية لشركة IBM. وقد توقف نظام شركة IBM تقريباً بسبب قيام هذا الفيروس بالتناسخ كلما وجد عنواناً يستطيع إرسال نفسه إليه. وتعرض نظام الشبكات Internet /Arpanet في الولايات المتحدة إلى عملية تحميل زائد مماثلة نتيجة برنامج لا يوجد فيه أي عامل تخريبي شرير.

يستطيع الفيروس ضمن محيط حوسبة ملائم مثل نظام نظيف أو شبكة حواسيب نظيفة نسخ نفسه مرات كثيرة جداً وبسرعة كبيرة. فيصبح الفيروس الواحد فجأة مئة أو ألف أو حتى ملايين من النسخ الفيروسية. والفيروس غير الضار قد يصبح هدّاماً بسبب عمل التناسخ هذا فقط بحيث يتمدد إلى حد يسد به النظام ويعطله نتيجة توالده مما لا يترك مجالاً لتنفيذ المهمات الأخرى.

السؤال رقم 5: لماذا من المهم والصعب إزالة الفيروس بالكامل من نظام ملوث؟

إذا تركت نسخة فيروسية واحدة في نظامك بعد انتهائك من عملية التطهير من الفيروس فإن هذه النسخة الفيروسية بإمكانها معاودة العمل والتناسخ معيدة نظامك إلى حالة تلوث كبيرة في غضون بضعة ثواني.

تذكر بأن الفيروسات قد لا تكون ظاهرة فقد تكون محجوبة ما بين أسطر من الشيفرة ومجزأة إلى أقسام صغيرة موزعة هنا وهناك ولكنها جاهزة للتجمع عندما تسنح الفرصة. والبعض منها يخبىء نفسه داخل القرص بحيث تبدو مثل «القطاعات السيئة» مما يجعل النظام أو البرنامج التطبيقي أو حتى البرامج الكاشفة للفيروسات لا تبحث في تلك القطاعات عن الشيفرة العادية أو الفيروسية. وهذه الأجزاء المتناثرة من شيفرة الفيروس شبيهة بحبات الرمل السوداء الملوثة بالنفط والمنتشرة على الرمل الأبيض على شاطىء جميل وهادىء. والشاطىء يبدو نظيفاً وعادياً ولكنه رغم ذلك يحتوي على عناصر هدامة خفية.

السؤال رقم 6: ما هي الأنظمة الأكثر عرضة للفيروسات؟

إن محيط تشغيل النظام DOS هو أكثر الأنظمة استعمالاً ولهذا فإن معظم حالات العدوى تحصل هناك. (إن نظامي تشغيل الحواسيب الشخصية الأكثر استعمالاً PC-DOS من شركة IBM و MS-DOS من Microsoft متشابهة كثيراً ولذا سوف تستعمل التعبير الإسمي DOS للإشارة إلى جميع أنظمة التشغيل المشتقة من النظام DOS لحواسيب شركة IBM أو ما يوافقها، والتي هي عرضة لنفس التأثيرات الفيروسية). والنظام DOS ليس فقط أكثر أنظمة التشغيل شيوعاً بل هو النظام الذي يجري فيه صنع الفيروسات.

أما أنظمة التشغيل الأخرى مثل OS/2 فإن ضعفها حيال الفيروس يزداد مع إزدياد استعمالها والسبب ليس فقط اتساع قاعدة تركيبها. فهنالك منحى متنامي نحو تطوير أنظمة مصممة لجذب اهتمام مستعملي شبكات الحواسيب مما يوفر المزيد من الشبكات لتنتشر فيها الفيروسات. واحدى حسنات النظام OS/2 وغيره من الأنظمة الجديدة احتواؤها على حواجز مبيتة ضد عدوى الفيروس ولكنها ليست كافية في الوقت الحاضر لجعل النظام OS/2 أو غيره منيعاً ضد الفيروس.

وعدد الأشخاص الذين يستعملون حواسيب الماكنتوش والاميغا والكومودور وغيرها من الأنظمة الامتلاكية أقل ولذا فإن محيطات الحوسبة هذه تعاني من عدد أقل من الفيروسات. وهذه الأنظمة لا تتمتع بنفس شعبية النظام DOS بالنسبة لصانعي الفيروسات. ورغم أن مالكي

أجهزة الماكنتوش يعتقدون بأن ليس لديهم مشكلة فيروس كبيرة فإن فيروسات الماكنتوش أكثر ضرراً من فيروسات أنظمة DOS وذلك لأن جميع البرامج التطبيقية للماكنتوش تعمل بنفس الطرق مما يوفر محيط عمل مريح لفيروس مصمم للتناسخ فيها.

ويعتبر نظام التشغيل CP/M الذي كان النظام القياسي للحواسيب الشخصية قبل النظام DOS، خالياً نسبياً من الفيروسات وذلك نظراً لتواجد عدد ضئيل جداً من البرامج الذاتية التناسخ عندما كان النظام CP/M شائع الاستعمال كما أن مهووسي الحواسيب انتقلوا إلى استعمال النظام DOS وما بعده. وإذا كنت خائفاً إلى حد الهوس من الفيروسات فإنك قد تشعر بالإطمئنان في محيط العمل CP/M حيث يوجد مجموعة كبيرة جداً من البرامج الجيدة والعتاد المستعمل الجيد يباع بأسعار زهيدة.

السؤال رقم 7: لماذا لا يهاجم الفيروس الحواسيب المتوسطة والحواسيب الإيوانية مثل الحواسيب الشخصية؟

الحواسيب المتوسطة (minicomputers) والحواسيب الإيوانية (mainframes) أقل عرضة للفيروسات لأسباب عديدة ولكنها عامل أساسي يساعد على نشر الفيروسات إلى الحواسيب الشخصية. غالباً ما تكون كلفة الحواسيب الكبيرة ملايين الدولارات وتكون عادةً مصممة إلى حد كبير بحيث تنفذ مهمات معينة بفعالية كبيرة. وبسبب هذا الاستثمار الكبير فإنها توضع عادةً في أماكن آمنة حيث لا يسمح بالدخول لأي كان. وهذه الأنظمة تملك وسائل أمن مبيتة ويجري حمايتها ضد جميع أنواع المخاطر طوال عمرها التشغيلي.

وهذا لا يجعل الحواسيب المتوسطة أو الأيوانية بمنأى عن الفيروسات بل هي أقل عرضة للتلوث وخاصة لأن معظم الفيروسات مصممة للنظام DOS ولذا لا تستطيع مهاجمة الحواسيب الأيوانية مباشرة. والأهداف الرئيسية للفيروسات هي آلاف الحواسيب الشخصية الموصولة بالحواسيب الأيوانية بطريقة أو بأخرى ولذا فإن كل ما تحتاجه الفيروسات للوصول إلى أهدافها هو المرور عبر الحاسوب الأيواني للوصول إلى الحواسيب الشخصية المتصلة بالشبكة. هنالك العديد من الأوبئة البشرية التي تستعمل أجساماً مضيفة للتنقل من ضحية إلى أخرى دون الإضرار بالمضيف أو الناقل الذي يوفر لها ملجأ مؤقتاً ووسيلة نقل مجانية.

اعتبرت علاقة فيروس النظام DOS مع الحواسيب الإيوانية مماثلة لاستعمال مجموعة من الإرهابيين لمحطة للسكة الحديدية كمركز لتوزيع القنابل. يأخذ زعيم المجموعة عدداً من القنابل إلى المحطة ويتركها في خزانة للحقائب. ويأتي بقية أفراد المجموعة بعد ذلك ويأخذون

القنابل ويستقلون قطارات مختلفة إلى المواقـع المستهدفة. وبعد فترة تحصل انفجارات متعددة في عدة مدن بعيدة، ولكن المحطة لا تتأثر ولا تتعرض لأي خطر في أي وقت من الأوقات. يمكنك اعتبار الحاسوب الإيواني مماثلاً لمحطة السكة الحديدية، والحواسيب الشخصية على أنها الأهداف البعيدة والفيروسات تلعب دور الإرهابيين المتنقلين الذين يحملون القنابل إلى الأهداف أو على أنهم القنابل نفسها، عاملين على إتلاف المعطيات عوضاً عن المباني.

ورغم عدم التلوث الفيروسي للحـواسيب المتوسـطة والحواسيب الإيوانيـة فـإن هذه الحواسيب الكبيرة تبقى تحدياً يحاول صانعو الفيروسات التصدي له. وهـم يقومون بكتابة فيروسات أكثر تطوراً وذكاءاً بإمكانها التأقلم مـع أنظمة تشغيل الحواسيب الإيوانية المختلفة وبناها والتغلب على إجراءات الأمن. وبانتشار اللغـات المستعملة في الحواسيب المتـوسطة والإيوانية فإن الوصول إلى هذه الحواسيب سوف يصبـح أسهل بالنسبة لصانعي الفيروسات ووسطاً مغرياً لكتابة الفيروسات.

تستطيـع الفيروسات أيضاً استغلال المزايا التخصصية لأنظمة الحواسيب الكبيرة. إذا أراد أحدهم تخريب نظام للحكومة أو لشركة كبيرة فإنه يستطيـع نشر فيروس بإمكانه التناسـخ بفعالية في أنظمة DOS ولكنه يبقى مختبئاً ولا يسبب الضرر إلا عندما ينتقل من محيط عمـل النظام DOS إلى الحاسوب المتوسط أو الإيواني المستهدف.

وهذه الاستراتيجية فعالة جداً لجميـع من يريد التسبب بضرر فادح لمجتمـع يعتمد على الحواسيب ومستعد للأنتظار. وبهذه الطريقة يتناسـخ الفيروس إلى حد يتزايد فيه مدى انتشاره في عالم الحوسبة بانتظام مما يزيد من احتمال قيامه في وقت ما وبطريقة ما بأيجاد طريقة إلى النظام المستهدف. وهذا نوع من الحرب الجرثومية الحاسوبية التي يتعرض فيها عدد كبير إلى الأذى. وأحد الأمثلة الأولى على مثل هذا النوع من الوسائل القادرة على ارتكاب هـذا النوع من التخريب الإلكتروني ضد الحكومات والمجتمعات التجارية والاكاديمية هو البرنامـج العدائي AIDS الذي ظهر لأول مرة في كانون الأول من العام 1989. (راجـع الفصل الثامن).

السؤال رقم 8: هل من الصعب صنـع الفيروسات؟

إن صعوبة صنـع الفيروسات تتضاءل يوماً بعد يوم! هنالك برامـج لصنـع الفيروسات تساعد من لا يملك خبرة في الحاسوب على صنـع الفيروسات بتوفير خيارات من قوائم تنتقي أقساماً كبيرة من شيفرات البرامـج. وهذا ينفي الحاجة إلى كتابة الكثير من شيفرة الفيروس الفعلية مما يفتـح الباب لإنشاء الفيروسات بسرعة وسهولة وبدون خبرة كبيرة. وهذا تطور مزعـج كثيراً.

وهنالك بعض الفيروسات التي يسهل صنعها دون مساعدة بينما يتطلب بعضها خبرة كبيرة في هندسة البرامج. ومع ازدياد نسبة اتقان الحواسيب فإن مئات الألوف من الأشخاص يملكون المعرفة الكافية لكتابة الفيروسات. والمحتم هو وجود دوافع شريرة ضمن هذا العدد المتزايد من المتضلعين في الحواسيب.

السؤال رقم 9: ماذا تستطيع الفيروسات عمله؟

لا حدود عملية لما يستطيع الفيروس عمله للتأثير على نشاط الحوسبة، وهو يتراوح من التسلية إلى الكارثة. وبعض النشاطات المتكتمة قد تؤدي إلى عواقب وخيمة لأن المستعمل قد لا ينتبه لفترة طويلة بأن عملاً سيئاً يحصل. وفي أسوأ الحالات فإن قدرة الفيروسات على إتلاف السجلات الطبية وأنظمة التحكم بحركة الطيران وغيرها من عمليات الحوسبة المهمة للسلامة يعني بأن هذه البرامج العدائية بإمكانها القتل فعلياً.

بإمكان الفيروسات تغيير قسم صغير فقط من المعطيات هنا وهناك مثل إضافة صفر لضرب بضعة أرقام بعشرة أو تحريك الفاصلة العشرية موضع أو موضعين بطريقة محتسبة أو عشوائية. أما في حالة الملفات النصية فيستطيع الفيروس تغيير الأسماء أو كلما ظهر اسم معين يرفقه بشتيمة. وهنالك فعلاً نوع من الفيروسات هدفه أنظمة معالجة الكلمات والتنقيح الإلكتروني والذي يضيف الشتائم إلى اسماء زعماء سياسيين معينين مثل الرئيس رونالد ريغان ورئيسة الوزراء مارغريت تاتشر والرئيس بيتر بوتا.

وليس من الصعب إنشاء فيروس يعمل على تغيير كلمات أو جمل معينة لتغيير المعنى، والتي لا ينتبه المستعمل إليها إلا بعد فوات الأوان. قد يكون من المضر كثيراً على سبيل المثال وضع الشتائم أو تغيير بعض الجمل أو إضافتها إلى مستنداتك خلال المرحلة من عملية معالجة الكلمات التي تقوم فيها بدمج البريد أو معالجة دفعة من الرسائل المعيارية. وافتقار هذه المرحلة إلى المراقبة البشرية قد يسمح بمرور عمل الفيروس دون الانتباه إليها إلا بعد وصولها إلى مستلمها بالطبع!

والإرسال الجماعي للبريد أصبح عملية روتينية بحيث أصبح بإمكان الفيروس المتخفي مثلاً، إضافة نص بعد كل مئة رسالة دون انتباه أحد. قد يقوم موظف مستاء أو مخرب يعمل لدى شركة منافسة بوضع فيروس يقوم بإضافة نص أولي يقول «بالطبع فإن جميع ما سبق هو أكاذيب». واحتمالات استغلال قدرة الفيروسات على تعديل النصوص والأرقام في الخفاء لا حصر لها وقد تكون مضرة جداً.

وتقوم بعض الفيروسات بإبطاء عمليات الحوسبة بسبب الحمل الذي يفرضه تكاثرها

وخاصة إذا كان هنالك علل في الفيروسات. ولكن يمكن جعلها تقوم بذلك عمداً بعدة طرق، وذلك إما للإزعاج أو لجعل النظام غير صالح للأستعمال. وقدرة التباطىء هذه قد تكون بهدف تخريب إحدى المنتوجات البراجية. مثلاً يمكنك جعل برنامج الصفحة المجدولة لمنافسك في السوق بطيئاً جداً عندما يغير خلايا الصفحة بحيث يزعج المستعمل ويفتح لك فرصة لتسويق برنامج الصفحات المجدولة الخاص بك.

ويمكن أيضاً استعمال الفيروسات لسرقة المعطيات والتي بدورها تساعد على سرقة ممتلكات محسوسة. مثلاً افترض بأن أحد مهووسي الحواسيب دخل عنوة في نظام لشركة وأنشأ حساباً خفياً أو مموهاً مما يفسح الفرصة لإدخال الفيروس. يستطيع الفيروس التجوال في النظام متناسخاً لزيادة قدرته على البحث في سجلات الدوائر المختلفة أو في نظام آخر قد يكون متصلاً مع الشبكة. تستطيع هذه النسخ الفيروسية تجميع معطيات خاصة عن الموظفين أو نتائج الأبحاث ومشاريع التطوير، أو خطط التسويق لمنتوج جديد أو المعادلات السرية، أو تفاصيل حول استراتيجيات الدمج والاستملاك أو غيرها من المعطيات المهمة وذلك دون معرفة أحد بذلك سوى الدخيل. وتنسخ هذه المعلومات بعد ذلك تلقائياً إلى الملف المخفي حيث يستطيع الدخيل تجميعه وتحليله كيفما يشاء.

وهذا يشبه السارق الذي يدخل عنوة إلى المقر الرئيسي لشركة ما ومن ثم يتحول إلى مئات السارقين الذين يبدأون بتفتيش خزائن الملفات والسجلات الخاصة في جميع أنحاء المبنى ناسخين جميع ما يهمهم دون المساس بالأصل بحيث لا يحس موظفو الشركة في اليوم التالي بأي شيء. وتؤخذ جميع هذه النسخ إلى زعيم العصابة الذي يرسلهم عبر الهاتف من المبنى إلى موقع معين في أي مكان من العالم.

وأحد الروتينات البسيطة التي يمكن برمجة برنامج الفيروس للقيام بها هو تنفيذ روتين عادي للنظام DOS في أسوأ وقت ممكن بحيث يلحق ضرراً فادحاً. مثلاً عندما تخزن أحد الملفات فقد يغير الفيروس الأمر إلى FORMAT (أمر النسق) الذي يتلف جميع المعطيات الموجودة على القرص الذي أردت حفظ عملك فيه.

وإضافة إلى تغيير الأوامر بإمكان الفيروسات إعادة تعريف المفاتيح نفسها التي تحاول بواسطتها إصدار الأمر. يستطيع النظام DOS وبعض البرامج التطبيقية جعل مفتاح الحرف «A» يعمل كمفتاح الحرف «Z». والعديد من البرامج التطبيقية تخولك إنشاء ماكروات يجري تشغيلها بمفتاح واحد بحيث تكبس على مفتاح واحد لإطلاق سلسلة من ضربات المفاتيح الكاملة. ويمكن برمجة الفيروس للقيام بجميع هذه الأعمال مشوشاً جدول تعريف ضربات المفاتيح أو منفذاً ماكروات هدامة.

تصور الفوضى والخسارة التي تتعرض لها مؤسسة كبيرة تملك شبكة حواسيب عند انتشار فيروس يعمل على تحويل لوحات المفاتيح QWERTY إلى الترتيب دفوراك. سوف يرتبك الضحايا ولن يتمكنوا من العمل وتتوقف عجلة العمل. عندما لا يعمل أحد المفاتيح بشكل جيد فإن المشكلة تكون سيئة مثلما يحصل عند سقوط رماد السجائر في لوحة المفاتيح ويسبب الأعطال، فكيف الحال عندما تتوقف جميع المفاتيح في جميع لوحات المفاتيح في جميع أنحاء الشبكة.

وهنالك أسلوب خادع آخر تستخدمه بعض الفيروسات هو تشويه جدول تخصيص الملفات FAT الذي يلعب دور فهرس النظام مبلغاً أياه عن مكان وجود الملفات المختلفة. يستطيع الفيروس أخذ كل هذه المعلومات وخلطها مثلما يحصل عند إلقاء بطاقات فهارس المكتبة على الأرض وإعادة تجميعها عشوائياً بحيث يصبح من المستحيل إيجاد كتاب معين وبالتالي جلبه من رف الكتب. وتستطيع بعض الفيروسات أيضاً تغيير غلافات جميع كتب المكتبة بحيث يصبح البحث عن كتاب معين اسوأ من البحث عن إبرة في كومة قش.

والفيروس هو أيضاً أداة اتصال فعالة عند برمجته لتوزيع الرسائل إلى نظام سيقوم بتلويثه. ولقد بدأنا نرى فيروسات تستعمل كوسائل دعائية مختلفة الأغراض تتراوح من الشعارات العنصرية إلى مساندة جعل المريجوانا قانونية كما يفعل فيروس نيوزيلندا الذي يعرض الرسالة:

Legalize marijuana. Your computer is now stoned.

السؤال رقم 10: هل يستطيع الفيروس الإضرار بالعتاد؟

تستقطب قدرة الفيروسات على الإضرار بالعتاد أو إلحاق أذى جسدي بالأشخاص اهتماماً كبيراً من أوساط الإعلام وقد جرى تضخيمها كثيراً. نظرياً يستطيع الفيروس جعل القرص الصلب في حاسوبك يدور بشكل متواصل إلى أن يتعطل أو يتعرض للاحماء الزائد أو يحترق ويحرق المبنى معه. ولكن هذا السيناريو مستبعد.

قد تتعرض بعض أنواع المراقيب إلى الضرر بسبب قيام الفيروس بالإرسال المتكرر لإشارة لامعة إلى أحد المواقع على الشاشة. هنالك طراز في الأقراص الصلبة من نوع معروف يميل إلى التعطل بسبب استعماله قطعة إلكترونية ضعيفة. ويمكن تخيل قيام أحدهم بكتابة فيروس يعمل على توليد أعمال كتابة وقراءة مكثفة تعجل في تعطل العتاد.

وفي الواقع من المستحيل بالنسبة للبراجيات بأن تعطل العتاد دون أن ينتبه المستعمل إلى وجود خطأ ما ذلك قبل حصول العطل الفعلي بوقت طويل. قد ينخفض العمر التشغيلي للقرص

الصلب بضعة مئات من الساعات نتيجة النشاط الفيروسي ولكن فقط إذا ترك القرص الصلب دون مراقبة لفترة طويلة من الوقت ولم يلاحظ أحدهم شيئاً.

الفيروسات ليست سوى نوع من البرامجيات ولذا فإنها تضر بالبرامجيات الأخرى أو المعطيات بشكل رئيسي. ولكن هذا الضرر سيء بحد ذاته وذلك لأن البرامجيات والمعطيات التي تنشئها قيمتها أكبر بكثير بالنسبة لمعظم مستعملي الحواسيب من الآلة المادية الفعلية.

بالطبع فإن الضرر المادي قد ينتج عن تلوث فيروسي للحواسيب التي تتحكم بالآلات. مثل رابوط التلحيم أو رابوط رش الدهان في مصنع تصنيع السيارات أو الأجهزة. ومثل هذه المعدات تشتمل على عدة إجراءات خالية من الأعطال بحيث تكتشف الشواذات في معطيات التحكم عادة. ولكن تلف معطيات التحكم قد لا تكون ظاهرة للعيان بسهولة في بعض الأعمال الحساسة مثل قياسات المكونات الداخلة في المنتوجات الكيميائية والأطعمة الجاهزة والأدوية والمواد الصيدلانية.

السؤال رقم 11: هل أصبح من الخطر استعمال البريد الإلكتروني؟

إن قدرة الفيروسات على الإضرار بالبريد الإلكتروني قد ضخمت كثيراً. وبما أن حركة الاتصالات هذه هي معطيات في اغلبيتها وليست معلومات برمجة، فإنها لا توفر للفيروسات سوى بضعة فرص قليلة وصعبة للاختباء أو لنشر العدوى.

وأنظمة البريد الإلكتروني التي لا ترسل المعطيات جيئة وذهاباً سوى على شكل نص وفق نظام الترميز ASCII هي آمنة نوعاً ما من خطر هذه الظاهرة المضرة. وخطر التلوث الكبير يتركز على الأنظمة التي تسمح بنقل الملفات القابلة للتنفيذ.

ورغم أن الفيروسات لا تستطيع تلويث المعطيات بل إتلافها أو تعديلها فقط فإنها تستطيع التنقل معها. فالفيروسات يمكن صنعها بحيث تحفز وتنقل نفسها عند فتح خط إلكتروني واستعمال البرامجيات لتنفيذ عملية نقل المعطيات. ورغم أن الفيروسات تلصق نفسها مع البرامج وتختبىء فيها فإن طبيعتها كبرامج تجعلها تحتوي على تعليمات تجعلها تنشر نفسها مع أنواع معينة من عمليات نقل المعطيات التي قد تحتوي شيفرة برمجة معينة.

السؤال رقم 12: ما هي أكثر فيروسات النظام DOS شيوعاً؟

القسم الأكبر من فيروسات النظام DOS تصنع كفيروسات تلوث قطاع الاستنهاض والتي تبحث عن الملفات COM. و EXE. . وهذه الملفات موجودة في جميع أنظمة DOS ولذا تصبح ضحية متوفرة وسهلة نسبياً. والملفات الجذابة للفيروسات بشكل خاص هي الملفات النظامية

المحجوبة وهي ملفات غير مسردة في دليل الملفات ولذا تلويثها أسهل دون كشف حالة التلويث (راجع الفصل الثاني والسادس).

يختبىء العديد من فيروسات النظام DOS في جهاز الساعة وذلك لأن هذا القسم من النظام يعمل حالما يوصل النظام بالطاقة. وبهذه الطريقة يجري تفعيل الفيروس قبل تمكن البرنامج المضاد للفيروس من البدء بفحص النظام. وهنالك عدة فيروسات تعمل على أساس الوقت وتحتوي على ما يشبه صمام التوقيت بحيث يقوم بمسح الساعة الداخلية لمعرفة عما إذا كان الوقت والتاريخ الحاليين يتفقان مع تعليماتها المبرمجة.

السؤال رقم 13: ما هي الفيروسات التي ينتهي عملها وتقيم في الذاكرة (TSR) ولماذا تثير المشاكل إلى هذا الحد؟

يبقى البرنامج نوع TSR في الذاكرة بعد قيامه بمهمة ما ويظل حاضراً للتنفيذ عندما يحتاج إليه. وتكون البرامج الغلافية (Shell) والساعات في أغلب الأحيان برامج من النوع TSR، وكذلك الأمر لبعض الفيروسات. حالما يدخل الفيروس في أحد الأنظمة ونفذ أعمال التلويث الأولية يقوم بالاختباء في الذاكرة RAM وينتظر فرصاً جديدة للتلويث مثلما يحصل مثلاً عندما تضع قرص في السواقة أو تتصل بحاسوب آخر على الشبكة. وحتى عند عدم تحفيزه فإن الفيروس نوع TSR بإمكانه التسبب بالأعطال نتيجة استحواذه على قسم من الذاكرة RAM مما قد يمنع بعض البرامج التطبيقية من العمل. وقد يتعارض الفيروس نوع TSR أيضاً مع البرامج بطرق أخرى وليس فقط عبر استحواذه للذاكرة RAM التي يحتاجونها.

وهذا النشاط الفيروسي ينشيء عوارض غريبة قد تلقي اللوم على علل البراجيات أو الأعطال العتادية مما يفسح في المجال للفيروس بأن ينتشر قبل اكتشافه.

السؤال رقم 14: هل أستطيع حماية نظامي ضد الفيروسات الموقوتة بضبط روزنامة وساعة حاسوبي عند وقت بعيد في المستقبل؟ أو هل استطيع أن أعيد الساعة إلى الوراء بحيث لا تقوم بتحفيز الفيروس؟

إن جهاز الساعة هو المخبأ المفضل للفيروس. وهذا الجزء من النظام يعمل عادة حالما يوصل النظام بالطاقة، ولذا قد يتم تحفيز الفيروس قبل أن يبدأ البرنامج المضاد للفيروس بالبحث عن النشاط الفيروسي. والفيروسات التي تمسح منطقة التخزين CMOS لمعرفة عما إذا كان الوقت والتاريخ الحاليين يطابقان الوقت والتاريخ اللذين برمجت لتعمل عندهما، أصبحت منتشرة كثيراً. وكذلك الأمر فإن الفيروسات التي تعدل وقت التحفيز أصبحت شائعة أيضاً

بحيث يتم جعل الفيروس يحفز عند الرابع من تموز/يوليو مثلاً ثم يجري تعديله ذاتياً بحيث ينطلق في الأول من تموز/يوليو بحيث يعدي عدد أكثر من الضحايا.

وبعض الخدع مثل تغيير تضبيطات الساعة والروزنامة قد تعمل في بعض الحالات ولكنها ليست بدفاع مناسب. فالفيروس الموقوت يضبط عادة ليحفز عند نقطة ما بعد تاريخ أو وقت معين بحيث قد تؤدي إلى اطلاقها بتقديم تضبيط الساعة والروزنامة.

السؤال رقم 15: كيف تستطيع الفيروسات منعك من الوصول إلى معطياتك رغم عدم إتلاف تلك المعطيات؟

هنالك طريقتان يتعرف بهما النظام DOS على الملفات والاثنتان معرضتان للهجوم الفيروسي. الأولى هي الترتيب المنطقي الذي تستطيع ضبطه بواسطة الأدلة والأدلة الفرعية والمسارات (paths) التي تجعل البرامج متوفرة بترتيب معين. وتجد الفيروسات أرضية مناسبة في الأدلة والأدلة الفرعية تستطيع فيها منع الوصول إلى الملفات بجعلها تبدو كما لو أنها قد اتلفت دون اتلافها فعلياً. وهذا النوع من الضرر يتطلب قدراً أقل من البرمجة بالمقارنة مع إتلاف سجلات المعطيات ولذا يجعل الفيروس متضام أكثر وبالتالي يصبح اكتشافه أصعب. وهي أيضاً طريقة لتمويه نشاط الفيروس بحيث لا ينتبه المستعمل إلى حالة العدوى. ورسالة عدم وجود الملف «File not found» قد لا تعني بأن المعطيات في المجال قد فقدت أو تلفت بل أن فيروساً قد قام بتغيير الدليل ليجعل من الصعب بل من المستحيل إيجاد موقع الملف.

نظام ترتيب الملفات الثاني هو جدول تخصيص الملفات FAT للنظام DOS، وهو الطريقة الغريبة وغير الفعالة غالباً التي يعتمدها النظام DOS لتخزين الملفات أجزاءاً متناثرة كلما وجد فسحة فارغة تستوعبها على القرص. فقد يجزىء أحد الملفات إلى أشلاء متناثرة في جميع أنحاء القرص ولا يعرف سوى الجدول FAT مكان تلك الأشلاء ويستطيع ضمان إيجاد وجمع تلك الاشلاء بالترتيب الصحيح إذا ما احتجتها. (وتستطيع ادراك طريقة عمل نظام التخزين هذا بالطريقة التي يدور فيها القرص الصلب محركاً الرأس جيئة وذهاباً لجمع جميع أجزاء الملف الطويل). وهذه العملية تستغرق وقت أطول كلما اكتظ القرص الصلب بسبب ازدياد حجم المعلومات التي يبحث فيها الجدول FAT ليتمكن من إيجاد عناصر الملف الذي يبحث عنه. وتوجد وسائل خدماتية للأقراص تقوم بإعادة ترتيب تلك الاشلاء بحيث تكون متجاورة مادياً قرب بعضها البعض لتسهيل عملية جمعها. والفيروس الذي يهاجم الجدول FAT يعيد ترتيب هذه الأمور ولكن بطريقة هدامة بحيث لا تستطيع إيجادها. (تستطيع بنفسك التسبب بنفس النتيجة الهدامة إذا استعملت وسيلة خدماتية تقوم بتعديل الجدول FAT استعمالاً خاطئاً).

السؤال رقم 16: كيف تستطيع فحص التدقيق التحذير بوجود عدوى فيروسية؟

فحص التدقيق (checksum) أو اللقطة (snapshot) كما يدعى أحياناً مماثل لبصمات الأصابع أو رقم الهوية لبرنامج أو ملف. وهو سجل عددي لحجم البرنامج أو الملف في حالته غير الملوثة ويمكنك استعمال ذلك كصورة مرجعية تستطيع التدقيق بها من وقت لآخر. وإذا تغير العدد فإن ذلك قد يشير إلى حصول عدوى فيروسية. وتقوم بعض البرامج المضادة للفيروسات أو الخدماتية بهذا العمل تلقائياً ونيابة عنك. ولكن بعض الفيروسات تقوم تلقائياً بتجاوز عملية فحص التدقيق لإخفاء وجودها.

السؤال رقم 17: لماذا تنشر ألواح الإعلان الفيروسات بهذا القدر؟

إن ألواح الإعلان (Bulletin boards) مثل الحفلات هي أماكن عظيمة للتعرف على أصدقاء جدد والحصول على معلومات والتقاط عدوى خبيثة إذا لم تكن حذراً. ويوجد حالياً في الولايات المتحدة أكثر من 30,000 لوح إعلان وينتظر ازدياد هذا الرقم كثيراً كلما تحسس الأفراد والمؤسسات الفائدة من إنشاء أمكنة الاجتماع الإلكترونية هذه. وقد كانت ألواح الإعلان حكراً على هواة الحوسبة. والآن تستطيع شركة صغيرة أو فرد واحد إنشاء لوح إعلان بكلفة وجهد ضئيلين. تستطيع في الولايات المتحدة بقدر من المال لا يزيد عن 50 دولاراً (أو حتى مجاناً إذا استعملت إحدى برامج المشاركة البرامجية أو العامة الممتازة المتوفرة) مع حاسوب شخصي بقرص صلب وخط هاتف، من إنشاء لوح إعلان وتشغيله بوقت قليل وبكلفة زهيدة جداً.

والمجتمع الاعمالي قد أصبح يعتمد أكثر وأكثر على ألواح الإعلان كطريقة للاتصال مع البائعين أو الموظفين الآخرين خارج المقر الرئيسي. وألواح الإعلان هي عنصر أساسي للمنحى المهم نحو الاتصال عن بعد (telecommuting). فمبدأ «الكوخ الإلكتروني» وغيره من أفكار محيط العمل المتغير يجعل من الممكن للموظفين إضافة إلى المقاولين المستقلين العمل انطلاقاً من منازلهم أو من مواقع بعيدة عن المرفق المركزي.

وألواح الإعلان أصبحت مهمة بالنسبة لمعظمنا تقريباً بعدة طرق. فهي سلعة رخيصة وكلما انخفضت الكلفة كلفاً ازدادت نسبة استعمالها. وبالفعل فإن ألواح الإعلان سوف تصبح وسيلة اتصال حيوية إلى حد يكفي أن تهددها الفيروسات فقط ليصبح أمامنا مشكلة خطيرة.

وبسبب هدفها المقتصر على استعمالها كوسط لتبادل المعطيات (وغالباً البرامج) فإن ألواح الإعلان معرضة لعدوى الفيروس. ولكن لا تدع وباء الفيروس يخيفك ويبعدك عن عالم ألواح الإعلان الرائع، كما حصل مع الكثير منا حين أصبحنا نخاف من الذهاب إلى حدائقنا العامة

والوسط التجاري لمدننا بعد حلول الظلام. يمكنك بنفس الطريقة التي تكون فيها حذراً ضمن المناطق السكنية، أن تكون حذراً عند استعمال خدمات غير مألوفة على لوح الإعلان.

السؤال رقم 18: لماذا لا يوجد لقاح عام ضد الفيروس لمنع العدوى، أو مضاد حيوي شامل يلتقط ويعالج التأثيرات المختلفة للفيروس؟

الجواب واضح إذا تذكرت بأن الفيروسات ليست بوجه جديد ومختلف لنشاطات الحوسبة بل مجرد برامج. وبالتالي فإنها تتصرف في عدة نواحي مثل البرامج العادية الصحية. ولذا فإن «الدواء» المصمم لإزالة الفيروسات قد يلحق الضرر بنشاطات الحوسبة العادية مثل مبيد الأعشاب الذي يقتل الأعشاب الضارة والنباتات المفيدة في آن. وكذلك الأمر فإن هذا «الدواء» يحتاج ليتمكن من اتلاف العدد الكبير من الفيروسات الموجودة أن يكون قوياً جداً بحيث قد يلحق الأذى بنظام الحوسبة، وذلك مثل بعض علاجات مرض السرطان والإيدز التي يصعب استعمالها لأنها تتلف الخلايا الجيدة إضافة إلى الخلايا الملوثة.

ولحسن الحظ فهنالك برامج مضادة للفيروس تقيم حلاً وسطاً ما بين هذه المستلزمات المتعارضة ولكنها تحتاج إلى التحديث الدائم. فالبرنامج المضاد للفيروس غير الحديث له نفس فائدة جرعة الانفلونزا في الموسم السابق. وشد الحبال ما بين أولئك الذين يصنعون الفيروسات واولئك الذين يحاولون هزيمتها هو صراع مستمر حيث يتوجب تعديل الأساليب الدفاعية تعديلاً متواصلاً لمواجهة الهجومات القادمة من كل حدب وصوب.

ولذا يجب أن تملك برنامجاً جديداً مضاداً للفيروسات أو واحداً يمكن تعديله بانتظام. والبرنامج VirusScan هو مثال على برنامج خدماتي يقوم بانتظام بقياس «درجة حرارة» نظامك ويبلغك عما إذا كان مريضاً ويحتاج إلى علاج.

السؤال رقم 19: لماذا تفقد السيطرة على الفيروسات المازحة أو غير الضارة لتقوم بأفعال لا يريدها من صنعها؟

الفيروسات هي براجيات ولذا فإنها قد تحتوي على علل (bugs) أو أخطاء في البرمجة مثل أي برنامج أخر. ويستحيل حتى على أكبر ناشري البراجيات الذين يملكون أساليب ووسائل اختبار غير محدودة من توليد برامج خالية كلياً من العلل. ويعتقد بعض الناشرين بأن برامجهم جيدة في حال كانت إصداراتهم الأولى لبرنامج جديد تحتوي على معدل خطأ أفضل من 3 بالمئة. ومبرمجو الفيروسات الذين يعملون غالباً بمفردهم بدون الوسائل التي يملكها الناشرون الكبار لفحص البرامج الجديدة، يملكون على الأرجح معدلات أخطاء أعلى تختلف حسب حجم وتعقيد البرنامج.

Converted by Tiff Combine - (no stamps are applied by registered version)

والعلاقة بين الفعل ورد الفعل لا تكون واضحة عادة وهذا يعقد الوضع أكثر. فالخطأ في أحد أجزاء البرنامج قد يؤدي إلى حصول خطأ في موقع مختلف كلياً. وردة الفعل أو التأثير في نظام معين يملك تشكيلة معينة من العتاد أو البرامجيات الخدماتية قد تكون مختلفة كلياً عن ما يحصل في نظام أخر.

وجميع الأخطاء في البرمجة قد تشكل عللاً تجعل البرنامج يقوم بأشياء لم يصمم للقيام بها. فالحاسوب يتطلب تعليمات دقيقة عكس الأنسان الذي يستطيع استخلاص المعنى الأساسي من المستندات التي قد تكون مليئة بأخطاء التهجئة والقواعد والتشكيل.

والعلل الموجودة في براجياتك حتى ولو كانت من صنف مشهور، قد تخلق عوارض شبيهة كثيراً بعدوى الفيروس. وإذا تعرضت لهجوم فيروسي في نظامك فإن العلل في برنامجها قد تخلق عوارض لم تظهر سابقاً في حالات العدوى بنفس الفيروس.

والعلل البراجية في البرامج العادية وفي الفيروسات تستطيع التسبب بفقدان المعطيات بعدة طرق قد تتراوح بين فقدان بضعة بايتات من المعلومات إلى اتلاف جميع المعطيات على القرص. واحياناً لا يجري سوى تشويه المعطيات مما قد يكون أكثر ضرراً من اتلافها كلياً إذا لم تكن تدرك ما يحصل. واحياناً أخرى قد تجعل العلل المعطيات تبدو وكأنها قد اتلفت بينما تكون في الواقع لا تزال موجودة وردة فعلك قد تجعلك تتلفها بنفسك.

وتحصل بعض العلل الفيروسية في أقسام تعليمات التسليم أو النسخ في البرنامج. وهذا قد يجعل الفيروس يضرب حاسوبات لم تكن في قائمة أهدافه كما حصل مع الفيروس Scores. فهذا الفيروس الذي يتفشى في حواسيب الماكنتوش كتب أصلاً لتلويث فقط تلك الأنظمة التي تشغل قواعد معطيات تقوم بمعالجة المعلومات خاصة بشركة Electronic Data Systems ولكن علة في الفيروس Scores جعلته يتفشى في جميع أنحاء محيط حوسبة الماكنتوش المرتبط بهذه الشركة، ليصل حتى إلى الأنظمة في وكالة الفضاء الأميركية ناسا ومجلس الشيوخ وحتى إلى حواسيب شركة آبل في مكاتبها في مدينة واشنطن.

وسببت إحدى العلل في الفيروس Jerusalem بجعل الفيروس يتناسخ بشكل جنوني معيداً تلويث الملفات التي سبق ولوثها. وقد كان لهذه العلة حسنات لأنها لفتت الأنظار إلى وجود خطأ ما قبل أن يتسنى لقسم اتلاف المعطيات في البرنامج من البدء بالعمل.

والعلة في البرنامج الدودي (worm) الذي اطلقه Robert Morris,Jr. في الشبكة البينية أدت إلى إزالة المكابح التي وضعها لمنع البرنامج من القيام بضرر فادح. وقد شق هذا الفيروس طريقه مثل القطار الهارب عبر شبكات وكالة الاتصالات لوزارة الدفاع الأميركية معطلاً

6000 نظاماً ومسبباً بأضرار مباشرة وغير مباشرة قدرتها الجمعية الصناعية لفيروسات الحواسيب (CVIA) بمبلغ مئة مليون دولار أميركي.

ومهووسو الحوسبة يتلذذون بإيجاد العلل في الفيروسات وتصحيحها، بحيث يجري ضبط وتحسين الفيروسات تباعاً خلال انتشارها في مجتمع الحوسبة وتتطور لتصبح أكثر فعالية مثلما تتابع البراجيات التجارية تحسنها من خلال إزالة عللها.

ولكن إزالة العلل من البرنامج الفيروسي أو تغيير البرنامج عمداً قد يؤدي إلى تعطيل الفكرة الأساسية والمنطق الداخلي للبرنامج. والعبث بالفيروس له مخاطر غير واضحة.

السؤال رقم 20: بما أن الفيروسات قد تنتقل إلى النسخ المساندة هل هنالك طريقة آمنة كلياً بإمكانها حماية المعطيات المهمة جيداً؟

نعم، ولكن وحتى تطوير وسيلة أفضل، فإن الحل الأفضل هو العودة إلى الأسلوب التقليدي في الطباعة على الورق. إذا كنت تملك معطيات يجب أن تحافظ عليها قم بطبعها بطريقة يسهل استخلاص المعلومات منها. ولا تستعمل بنوطاً ونسقاً تزينية بل قم بإعداد نسخة مطبوعة مستخدماً نوع الحرف والترتيب الذي يمكن قراءته بدقة من قبل أجهزة المسح الضوئي المتعددة المتوفرة.

ولا يحتاج حتى إلى امتلاك ماسح (Scanner) بل حضّر نسخ مطبوعة ارشيفية بنسق مناسب واحفظها بطريقة آمنة كما يشرح الفصل العاشر. وعند ذلك وإذا خسرت جميع معطيات حاسوبك بسبب تلوث فيروسي أو لسبب أخر تستطيع استعمال النسخ المطبوعة وجعل أحدهم يمسحها لك أو تشتري ماسحاً عند ذلك الوقت. وكلفة هذه المعدات تكلف 200 دولار أميركي فقط والذي سوف يبدو مبلغاً زهيداً عندما ترى عودة النسخ المطبوعة إلى شكلها الإلكتروني وتسترد بالتالي المعطيات التي كنت سوف تخسرها، صحيحة وجاهزة للمعالجة عن جديد.

4 أمثلة على بعض أنواع الفيروسات

يحتوي هذا الفصل على أوصاف لبعض البرامج الفيروسية. وسوف تشرح ستة فيروسات، ثلاثة منها يتميزان بنوعين من العروض.

الفيروس التعاقبي Cascade Virus

تسقط المحارف في هذا الفيروس التعاقبي عمودياً على الشاشة إلى أن تصادف محرفاً آخر أو تغيراً في ألوان الجهة الخلفية أو الأمامية.

والمنطقة التي تتأثر على الشاشة هي عمود واحد مبدئياً. ولكن التأثير يتراكم بعروضات متلاحقة إلى أن تتأثر الشاشة باكملها. والتأخير الزمني قبل بدء العرض الأول عشوائي وقد يصل إلى خمسة دقائق. أما التأخيرات الزمنية اللاحقة ما بين العروضات فعشوائية أيضاً وتصل إلى دقيقة واحدة.

فيروس دنزوك ـ Denzuk Virus

هذا العرض الواحد ليس ببرنامج من النوع الذي ينتهي ويقيم في الذاكرة (TSR) كما يعمل بلا بارامترات. وهو يعرض الكلمة DENZUK بشكل استعراضي عند الكبس على التوليفة Ctrl-Alt-Del لاستنهاض الحاسوب.

فيروس فومانشو ـ Fu Manchu Virus

يعترض هذا الفيروس طلب مقاطعة الدخل/الخرج للوحة المفاتيح (الطريقة التي ترسل بها أفعال لوحة المفاتيح إلى الحاسوب للمعالجة). وعندما يتعرف الفيروس على كلمات معينة يقوم بإضافة ملاحظات إليها.

والكلمات المحفزة تشمل «Thatcher» و«Botha» و«Reagan» و«Waldheim» و«Fu Manchu». وتكون الكلمة (أو الكلمات) يليها فسحة فارغة هي الحافز. أما الكلمات المحفزة الأخرى فهي كلمتين بذيئتين (لا يتبعها فسحة فارغة). ويجري اعتراض التوليفة Ctrl-Alt-Del وتظهر رسالة قبل إعادة استنهاض الحاسوب.

الفيروس الإيطالي - Italian Virus

يؤدي هذا الفيروس إلى جعل إحدى المحارف تصبح «كرة مرتدة» على الشاشة. وتأثيره مماثل للعبة كرة الطاولة الإلكترونية وغيرها من برامج الكرات المرتدة المنتشرة كثيراً ما بين الحواسيب وأنظمة التشغيل المختلفة.

ويتحفز العرض عندما تحاول الوصول إلى القرص بحيث تعرض «نافذة» تدوم لمدة ثانية واحدة كل نصف ساعة.

فيروس القدس - Jerusalem Virus

بعد حصول تأخير زمني أولي يتدرج قسم من الشاشة إلى الأعلى مقدار سطرين مما ينشىء فجوة صغيرة وسوداء في العرض. وبنفس الوقت يتم تشغيل حلقة تكرار لتضييع الوقت ويبدو كما لو أن المعالج أصبح بطيئاً.

الفيروس الموسيقي أوروباكس - Oropax Musical Virus

لقد غاب عن الفيروسات لمدة طويلة التأثيرات الصوتية أو كانت بدائية جداً إلى أن ظهر الفيروس أوروباكس وهو فيروس يلوث البرامج التطبيقية بدأ بالانتشار في أوروبا والولايات المتحدة في العام 1990. ويؤدي هذا الفيروس مقطوعات موسيقية مثل النشيد الوطني الأميركي أو الدانوب الأزرق أو إحدى مقطوعات موزارت.

5 الفيروسات ليست سبب المشاكل دائماً

لقد ازدادت خلال الثمانينات قيمة ووثوقية الحواسيب كثيراً. ومع انخفاض أسعارها انخفضت أيضاً معدلات التعطل مع تحسين الدوائر الكهربائية والأجزاء الميكانيكية القليلة في الحواسيب الشخصية.

أما في التسعينات فإن سرعة التحسين سوف تنخفض كثيراً. وقدرة الحوسبة التي تحصل عليها لقاء ما تدفعه من مال سوف تواصل ازديادها ولكن ليس بنفس السرعة التي عشناها في الثمانينات وذلك بسبب العوامل التوفيرية التي تخضع لها أسعار المبيع. ووثوقية الأجهزة أصبحت جيدة الآن إلى حد لم يعد هنالك من مجال للتحسين في هذا الحقل. ولكن هذا التباطؤ سوف يتوقف ليعود النشاط المتزايد إلى الأنظمة كلما خفت حدة نشاط الفيروسات بسبب التطور والتقدم في تصميم وصناعة العتاد.

ونتوقع التوقف الكلي للمزيد من البرامج، وخسارة المعطيات وتعطل العتاد مع انتشار الفيروسات وقيامها بعملها القذر في المزيد من الأنظمة. ولكن لا تدع الواقع الذي يشير إلى أنه رغم تحسن العتاد فإن الفيروسات قد أصبحت اسوأ، يجعلك تحزن بلا سبب وتعرض نفسك للإرهاق الفكري لاعتقادك بأن نظامك قد تلوث كلما حصل عطل ما. إذا اتخذت إجراءات احترازية معقولة لإبعاد الفيروسات عن نظامك فإن احتمال نشوء المشكلة بسبب علة في البرنامج أو عطل في العتاد أكبر من نشوئها بسبب الفيروس.

وفي الواقع وإذا نظرت من حولك في مكتبك فإنك قد تشاهد مخاطر وضعتها بنفسك في محيط عملك تشكل خطراً أكبر من عدوى الفيروس. وكما أن الفيروس هو مشكلة بشرية فكذلك هي الأسباب الأخرى لتعطل الحواسيب.

عادات البرمجة السيئة

لو كان هنالك وكالة لحماية البيئة بالنسبة للحواسيب فإنها قد تعطى لائحة لمستعملي الحواسيب تشمل الأسئلة التالية المتعلقة بمكان عملهم:

- هل كان القرص الذي استعملته لتوك متكئاً على الهاتف أو ملقى على المرقاب؟
- هل تحتفظ بمشابك الورق بالقرب منك داخل إحدى تلك العلب الصغيرة الذكية التصميم الممغنطة من الأعلى؟
- هل قمت بنفض الغبار من مكان عملك مؤخراً؟
- أين تضع كوب قهوتك؟
- هل تدخن أو تأكل الفشار أو المكسرات أو رقائق البطاطس قرب حاسوبك؟
- هل تمر أشعة الشمس عبر نافذة قريبة؟
- هل الأقراص ملقاة فوق بعضها البعض؟
- هل الثلاجة أو السخان الكهربائي أو الغسالة أو مكيف الهواء موصولة على نفس الخط الكهربائي الذي يتصل به حاسوبك؟
- هل الكبلات ملفوفة معاً بشكل مرتب؟
- هل يوجد سجادة مريحة على الأرض؟

إذا أجبت بالإيجاب على إحدى هذه الأسئلة فإنك تكون تعرض معطياتك إلى خطر أكبر من أي خطر قد تعرضها له عند استعمال أكثر ألواح الإعلان خطراً. وتدل جميع هذه الأسئلة على أساليب عمل غير آمنة للحوسبة قد تؤدي إلى عوارض يصعب تمييزها في البداية عن عوارض هجوم الفيروس.

دعونا الآن نعاين مخاطر مكان عمل الحاسوب هذه بتفصيل أكبر.

هل كان القرص الذي استعملته لتوك متكئاً على الهاتف أو ملقى على المرقاب؟ هل تحتفظ بمشابك الورق بالقرب منك داخل إحدى تلك العلب الصغيرة الذكية التصميم الممغنطة من الأعلى.

بما أن البرامج والمعطيات تخزن بواسطة المغنطة المضبطة فإنها قد تتعرض للتلف نتيجة المجالات المغنطيسية العشوائية التي يوجد الكثير منها في المكتب أو المنزل النموذجي.

هنالك الملايين من المغنطيسات الصغيرة في القرص المرن وحتى أضعف المجالات المغنطيسية بإمكانه تشويه التراصف التام لهذه المغنطيسيات المجهرية الضروري للمحافظة على دقة المعطيات. مثلاً، المغنطيس في الهاتف يولد مجالات مغنطيسية قوية جداً عندما يشتغل نتيجة مخابرة داخلة. والمعطيات المهمة المخزونة على القرص يمكن أن تتلف أو تشوه في لحظة إذا كان القرص قريباً من الهاتف لحظة رنينه.

حاويات مشابك الورق هي سبب آخر لفقدان المعطيات ويجب عدم وضعها إطلاقاً على المنضدة حيث يوضع نظام الحاسوب. إذا كنت تملك إحدى حاملات النسخ التي تملك مشبكاً مغنطيسياً لإبقاء الأوراق منتظمة تخلص منها فوراً فإنها تهدد صحة معطياتك. والمستغرب هو بيع هذه الأشياء في مخازن مشهورة اختصاصها لوازم الحواسيب ولكن هذا ليس أسوأ مثال على الجهل المتعلق بالأذى الناتج عن تفاعل المغنطيس والأقراص. فأحد ناشري البرامجيات الذي ينتظر منه معرفة هذه الأمور، قام بإرسال قرص تجريبي وارفق معه بنفس الرزمة حاملة أوراق مغنطيسية. وقد يكون ذلك أول حالة لبريد ذاتي التلف!.

ومسجلات الأشرطة وبالأخص النوع الجيبي الذي يحمله معظمنا لتسجيل الملاحظات والتي نحتاجها على مكاتبنا قد تختبىء بسهولة تحت كومة من الأوراق. والمجال المغنطيسي الذي يولده الميكروفون أو المجهار في مسجل الأشرطة قد يكون قوياً إلى درجة يؤدي فيها إلى ضرر كبير على الأقراص الموجودة في الجوار. وإذا تأذى القرص فقد لا تلاحظ المعطيات المشوهة أو البرمجة المشوشة لفترة طويلة ولذا لا يقام رابط ما بين الفعل وردة الفعل. وفي هذه الحالة يمكن الشك بالفيروس وتتم إضاعة وقت كبير في محاولة تتبع العدوى غير الموجودة أصلاً.

وبعض المصادر المغنطيسية في مكان عملك هي المرقاب (وخاصة إذا كان مرقاب ملون)، والطابعة ومكبرات الصوت والهواتف المزودة بمكبرات صوت والآلات الكاتبة الكهربائية ومصابيح المكتب (وخاصة الفلورية منها المزودة بكابح تيار).

هل قمت بنفض الغبار من مكان عملك مؤخراً؟

إذا فعلت ذلك فإنك تكون على الأرجح قد زدت من مخاطر سوء أداء نظامك لأسباب ميكانيكية. الغبار هو العدو رقم 1 للشعب فيما يختص بالمعطيات وهو مهلك للأقراص في حال تواجده بكثرة.

الاستعمال غير المتأني لمنفضة الغبار أو المكنسة أو المكنسة الكهربائية حول موقع عمل الحاسوب بإمكانه نشر جزيئات الغبار والشعر ورماد السجائر على أسطح الأقراص ورؤوس القراءة/الكتابة مسبباً أضراراً مادية واخطاء عند القراءة. وتتفاقم المشكلة أكثر عندما تنفصل جزيئات من الأوكسيد عن سطح القرص مسببة بالمزيد من التلوث.

وقدرة تحمل القرص للهجومات المادية للغبار وغيره من المواد الملوثة للجو يعتمد على نوعية تصنيعه ومدى استعماله وسوء استعماله. الأقراص المنخفضة النوعية تحتوي على طبقات رقيقة من الأوكسيد بحيث تنفصل بسهولة (يتناسب معدل تفتت سطح القرص عادةً بشكل

عكسي مـع كلفة القرص) ويوجد عادةً بطانة قماشية منخفضة النوعية في الدثار الذي يحيط بالقرص. ويفترض أن تلتقط البطانة نتف الأوكسيد المولدة في الداخل إضافة إلى الغبار الذي يخترق الدفاعات الخارجية المتمثلة بالدثار أو الغلاف.. وفي الظروف السيئة وخاصة في حالة الأقراص المتدنية النوعية تصبـح البطانة مشبعة بالجزيئات والغبار إلى حد لا تعد تعمل جيداً كما الحال مـع مرشـح الهواء في المحرك الذي قد يسد. وهكذا وعوضاً عن قيام البطانة بتنظيف القرص يتأتى عن ذلك عملية احتكاك خلال دوران القرص وتنتشر القمامة الفتاكة على الرؤوس وعلى الأقراص الأخرى. ومشاكل القراءة والكتابة التي تختص بها بعض الفيروسات قد يكون سببها هو التلوث بالغبار والأوساخ في سواقـات الأقراص. وقـد يتلف قسم من السطـح الأوكسيدي إلى حد لا يمكن عنده تخزين المعطيات أو استردادها مما يؤدي إلى ظاهرة «هبوط» (لا يعد فيها من الممكن الوصول إلى أقسام من القرص). وهذه الظاهرة تشبه إلى حد كبير عوارض الفيروس.

إذا كنت تستعمل إحدى محززات الأقراص (disk notcher) التي تخولك الوصول إلى الجانب الآخر لقرص آحادي الجوانب فإنك تزيد من الخطر المادي. ويعمل المحزز بقطـع قطعة صغيرة من حافة غطاء القرص بحيث لا يعد القرص محمي ضد الكتابة. وقد تبدو الآلة وكأنها قامت بعمل جيد وخالي من الشوائب ولكن قد تتناثر نتفاً صغيرة من القرص وتلتصق بسطـح القرص. واستعمال الجانب الآخر للقرص يتطلب وضعه في السواقة مقلوباً. وهذا يعكس اتجاه دورانه ويسلط ضغطاً على السطـح الممغنط للبطانة مما يزيد من احتمال انفصال الغبار وغيره من الأوساخ عن البطانة وسقوطها على سطـح القرص. وقد يحصل تلف استنزافي للمعطيات أيضاً حيث تنزف القوى المغنطيسية التي تنشؤها عملية تخزين المعطيات، على أحد الجوانب إلى الجانب الآخر لتؤثر على معطيات الجانب الآخر.

وبصمات الأصابـع هي سبب آخر من أسباب سوء أداء الأقراص. فلا يجب إطلاقاً لمس السطـح المغطى بالأوكسيـد مباشرة ويجب الإمساك بالأقراص من دثارها الخارجي. ويحصل أن تلمس أسطـح الأقراص دون قصد ولكن معظم المشاكل تنتـج عن العمل غير المنظم أو عن عادات متأصلة. وفتـح المغلاق المعدني الصغير على الأقراص الصغيرة واغلاقها قد أصبـح من العادات الحديثة في هذا العصر العالي التقانة وقد حل محل عادةً ثني مشابك الورق.

والأفضل إتباع عادة بناءة هي وضـع الأقراص في ظروفها الورقية كلما كانت خارج السواقة وتكديسها عمودياً في علبة غير معدنية تحميها من الغبار وغيره من مخاطر البيئة. والتكديس العمودي مهم لأنه يخفف من احتمال حصول ضرر مادي أو دخول الغبار. وتميل الأقراص الملقاة هنا وهناك بشكل غير مرتب أكثر إلى احتمال تعرضها للإنثناء أو وضـع أغراض

عليها مما يؤدي إلى تلامس البطانة والقرص معاً. وجميع أسباب الضرر المادي هذه تؤدي إلى عوارض مماثلة للضرر الإلكتروني الذي تسببه بعض التلوثات الفيروسية.

ووسط التخزين الممغنط هو عرضة بدوره للأذى. وعندما يصادف الحاسوب قطاعاً سيئاً على القرص فإنه لا يستطيع إبلاغك عما إذا كان الضرر ناتج عن فيروس يعيث الفساد في نظامك أو أن المستعمل قد استعمل قلماً برأس كروي صلب عوضاً عن قلم برأس لبادي طري للكتابة على اللصيقة المثبتة على القرص. لا تأتي اللصيقات والأقراص كل على حدى لتوفير كلفة التصنيع!.

وقد يساهم تراكم الغبار داخل الحاسوب أو الطابعة أيضاً في حصول مشاكل الإحماء الزائد أو الكهرباء الساكنة وتقصير الدوائر الكهربائية وتعطل الرقائق وغيرها من المآسي التشغيلية التي قد تعطي نفس عوارض التلوث الفيروسي، وخاصة إذا كانت المشكلة متقطعة. تعمل المراقيب وغيرها من المكونات الكهربائية المشحونة شحنات عالية كجاذبات للغبار وغيرها من الجزيئات ولذا فإن القيام بأعمال تنظيف داخلية دورية لحاسوبك واجهزته المساعدة مهم جداً.

وإبقاء المنطقة حول حاسوبك نظيفة ضروري، فعندما يتسخ موقع عملك نظفه بقطعة قماش أو اسفنجة رطبة وليس بنفض الغبار بقوة. ويمكن التحكم بمقدار الغبار بفعالية أكبر عند استعمال مادة رش مضادة للكهرباء الساكنة بعناية، مثل محلول بنسبة 20 بالمئة من مادة لتطرية القماش ومسح الأسطح الخارجية لحاويات العتاد. وفي حالات العمل الكثيرة الغبار فإن وضع أغطية من البلاستيك أو القماش على العتاد ضروري. ولقد أنقذ نظامي بأكمله في أحد المرات بواسطة أغطية الغبار البلاستيكية الهزيلة التي استعملها. فقد كنت خارج المنزل طوال عطلة الأسبوع عندما حصل تسرب في سقف منزلي نتيجة عاصفة قوية وبدأ الماء بالتقطر عبر السقف وعلى مكتبي. ولقد أتلفت الماء النسخ المطبوعة ولكن حاسوبي والمعطيات المخزونة فيه بقت جافة تحت خيمها الصغيرة الزهيدة الثمن.

عندما تخفق سواقات الأقراص (وخاصة في الأنظمة القديمة) بالقراءة من القرص أو الكتابة عليه فقد يكون السبب وجود أوساخ فيها. وازالتها ومنعها من الحصول مجدداً قد يكون أسهل من محاولة إيجاد عدوى فيروسية غير موجودة. والتنظيف اليدوي لرؤوس القراءة والكتابة ليس بالصعوبة التي قد تتخيلها ولكن لا تحاول تغميس قطيلة في سائل كحولي وادخالها عبر شقب السواقة آملاً بأن تزيل الأوساخ التي تسبب المشاكل. وهذا الأمر ليس بمزحة فقد اضطررت منذ عدة سنوات القيام بهذا العمل مع النظام CP/M القديم الذي كنت أملكه في موقع عمل في أفريقيا حيث لا يوجد المواد أو الخدمات الضرورية. وقد أصلح ذلك العطل بسرعة ولكن من الأفضل لو استعملت طقم التصليح المناسب المزود بقطيلات خالية من النسالة ومحلول كحولي

مخفف أو مادة مذيبة خاصة. وإذا قررت تنظيف رؤوس القراءة والكتابة فقد تحتاج إلى تفكيك قسم من الحاسوب والسواقات للقيام بالتنظيف اليدوي والتي لا يجب القيام بها دون معرفة فنية أو دون وجود دليل جيد يعطيك تعليمات مفصلة وتدريجية.

والطريقة الأسهل لتنظيف داخل سواقات الأقراص (رغم أنها لا تعطي نفس النظافة الكاملة كطقم التنظيف اليدوي) هو وضع قرص خاص بتنظيف الرؤوس في النظام. أنتق نوعاً موثوقاً وغير حاك. واتبع التعليمات بحذافيرها مع الانتباه بشكل خاص إلى طريقة وضع المادة المذيبة والوقت. والواجب تشغيل القرص عنده. واستعمال القليل أو الكثير من المادة المذيبة وترك القرص لأكثر من 15 إلى 20 ثانية أكثر من اللزوم قد يلحق أذى أكبر من الأذى الذي قد يحصل عند عدم التنظيف.

ويختلف الخبراء حول وجوب استعمال منظفات الأقراص كدواء وقائي. وسهولة استعمالها يجعل من غير الصعب استعمالها أسبوعياً أو شهرياً أو ثلاث مرات في السنة بناءاً على توصيات الشركة المصنعة ومدى استعمال الحاسوب. وأنا شخصياً من اتباع النهج الذي يقول بترك الأقراص في الحالات العادية والانتظار حتى حصول أخطاء في الكتابة والقراءة قبل تنظيف الرؤوس.

كلمة أخيرة حول سواقات الأقراص: لا تهتم كثيراً للأصوات الغريبة الصادرة عنها. قد تسبب بعض الفيروسات بحصول نشاط جنوني في الأقراص وهذا سبب يدعو إلى الاهتمام خاصة إذا كان الوقت المطلوب من القرص لينفذ مهمة ما احتاج إلى وقت طويل جداً. ولكن غالباً ما يدور ويزمجر القرص بطريقة ملفتة للانتباه دون أن يكون هنالك عطل ما. وقد تلاحظ بأن بعض أنواع سواقات الأقراص المرنة أكثر ضجيجاً من غيرها وهذا ليس عيباً. فالصوت قد يشير إلى أن البطانة تعمل بفعالية على إبقاء السطح الأوكسيدي نظيفاً بينما بعض الأقراص قد تبدو أقل ضجيجاً لمجرد أنها تملك بطانة أقل فعالية.

تسبب الأقلام والأقلام الكروية الرأس والأصابع اللزجة وحاويات مشابك الورق الممغنطة والغبار بأضرار لمعطيات الأقراص أكثر من الأعداد ذوي التقانة العالية مثل فيروسات الحواسيب وآلات الأشعة السينية في نقاط التفتيش في المطارات. وفي الواقع فإن الأشعة السينية لا تسبب على الأرجح أي ضرر في الظروف العادية رغم أنه من الأفضل تجنب التعرض المتكرر للأشعة السينية التي قد تحصل في الرحلات الطويلة حيث يتم التوقف في عدة مطارات فقد يؤدي ذلك إلى تأثير متراكم ضار مماثل لذلك الذي يؤدي إلى حصول ضبابية في الأفلام الفوتوغرافية. وقد تكون آلات الأشعة السينية مضبطة ضبطاً غير صحيح في بعض البلدان أو أنها تولد إشعاعات قوية مما قد يشوه المعطيات المرقمة وبالتالي إستحداث عوارض شبيهة بالعدوى الفيروسية.

أين تضع كوب قهوتك؟ هل تدخن أو تأكل الفشار أو المكسرات أو رقائق البطاطا قرب حاسوبك؟

يعاني المدخنون عموماً المزيد من المشاكل مع معالجة المعطيات أكثر مما يعانيه غير المدخنين لأن رماد السجائر والغليون والسيجار يؤدي إلى إزدياد كبير في حجم الجزيئات الموجودة في الهواء والتي قد تترسب على أسطح الأقراص والقطع الإلكترونية.

ومادة القطران الموجودة في الدخان تدخل أيضاً في جميع الأمكنة وتتجمع مع الرماد والغبار لتشكيل صمغ كيميائي قد لا يكون مستفحلاً إلى حد يمكن رؤيته ولكن لديه المقدرة على إتلاف المعطيات خلال عمليات القراءة والكتابة.

ورغم احتمال سكب القهوة أوغيرها من السوائل على الأقراص واضح فإن لوحة المفاتيح هي أكثر القطع تعرضاً للإتساخ. والنتف المتطايرة نتيجة أكل الطعام بالقرب من الشاشة قد يؤدي أيضاً إلى تلوث لوحة المفاتيح.

وقد تباهى أحد الفنيين أمامي قائلاً، «أستطيع معرفة الكثير عن العادات الشخصية ونوع غذاء مستعمل الحاسوب عندما أنظف لوحة المفاتيح».

ولقد اقتنعت مؤخراً بأنني قد التقطت عدوى فيروسي معين لأنه للمرة الأولى منذ ثلاث سنوات توقفت لوحة مفاتيحي عن العمل كما يجب وبدأت تفقد بعض الأحرف بطريقة يمكن برمجة الفيروس ليقوم بها. وقد استعملت البرنامج VirusScan الذي أعطى الحاسوب شهادة صحية ولذا أخذت مفك البراغي وفككت لوحة المفاتيح مما أظهر تلوثاً بالأوساخ ورغوة المعادن منع بعض المفاتيح من التلامس بشكل صحيح. والسبب الرئيسي للتلوث كان نتف من الفشار!.

وليس من الصعب تفكيك معظم لوحات المفاتيح. إفصل لوحة المفاتيح عن النظام واقلبها رأساً على عقب وانزع اللوالب. (تحذير: يؤدي هذا حتماً إلى إلغاء كفالة حاسوبك). إفصل نصفي الغلاف البلاستيكي الخارجي على مهل للوصول إلى المفاتيح والدوائر الإلكترونية الداخلية. يمكن إزالة الحتات من المفاتيح والدوائر بنفخها بهواء مضغوط أوسحبها برفق بواسطة مكنسة كهربائية أو إزالتها بالفرشاة. ولقد نظفت لوحة مفاتيحي بمكنسة كهربائية من النوع الصغير العامل على البطارية وبفرشاة لمستحضرات التجميل من النوع الناعم جداً والزهيدة الثمن. واستعمل منذ ذلك الوقت المكنسة الكهربائية الصغيرة والفرشاة لتنظيف لوحة المفاتيح من الخارج لالتقاط الحتات قبل دخوله ما بين المفاتيح. وهذا علاج وقائي للحواسيب النقالة التي قد تتعرض أكثر من غيرها لالتقاط المواد الغريبة وتملك لوحة مفاتيح يصعب على المستعمل وحتى يستحيل عليه فكها لتنظيفها.

والفأرة (mouse) التي أصبحت أداة مساعدة متزايدة الشعبية والتي انتشرت كثيراً خارج بيئة الماكنتوش الأصلية تتميز ببرمجة قد تكون هدفاً لصانعي الفيروسات. ولكن إذا بدأت الفأرة بالتصرف بغرابة فإن السبب ليس بالضرورة الفيروس. فبعد تحركها عدة أميال على لوحتها على المكتب قد تلتقط الفأرة كثيراً من الأوساخ وغيرها من الملوثات بحيث يلتصب نظامها الميكانيكي. إعمل دورياً على فك الفأرة وتنظيفها للحصول على أداء سلس وموثوق.

هل تمر أشعة الشمس عبر نافذة قريبة؟

إذا كانت أشعة الشمس واقعة على أقراص القيتها على مكتبك فإنها قد تلتوي بسرعة أو تتمدد إلى حد يؤدي إلى مشاكل في القراءة والكتابة قد يتهم بها الفيروس. ويكفي قدر صغير من التعرض للحرارة لجعل القرص عديم الفائدة.

والالتواء الذي يمنع القرص من الدوران داخل غلافه هو واحد من العواقب الواضحة. حتى وإن بدا القرص جيداً ويمكن وضعه وتشغيله في النظام فإن التمدد الحراري قد يغير موقع المعلومات فيه، فالمعطيات تخزن بنسبة 10 بايتات في كل 0.001 إنش مربع على سطح القرص ولذا لا يحتاج الأمر إلى الكثير من الإزاحة لتشويه المعطيات المخزونة.

ويمكن أن ينتُج بعض أكثر التصرفات السيئة غموضاً وشبهاً للفيروس في النظام من جراء نوع آخر من الضرر الحراري للعتاد. فترك الورق فوق فتحات التهوية على حاسوب الماكنتوش أو جعل الحاسوب الشخصي (PC) أو الأميغا أو الكومودور تحمى كثيراً قد يؤدي إلى مجموعة مدهشة من المشاكل التي تتحدى العديد من الاختبارات التشخيصية التقليدية للعتاد السيّىء الأداء.

ورغم أن حواسيب الماكنتوش لا تملك مراوح تهوية فإنها تتأقلم جيداً مع حالات الحرارة، بينما الحواسيب الشخصية رغم تبريدها القسري بالمروحة قد تكون ضعيفة وحساسة جداً. وينشأ الكثير من مشاكل التبريد نتيجة إضافة لوحات توسيع وغيرها من الدوائر إلى أنظمة الحواسيب الشخصية. وسرعان ما يمتلىء داخل العلبة بقطع زائدة تنتج جميعها الحرارة مما يزيد في العمل على مصدر الطاقة الكهربائية ويعيق انسياب الهواء.

ودرجات الحرارة العالية تعني تلف أسرع للأجزاء المكونة ولذا تبدأ الرقائق بالعمل بشكل غير منتظم وتنشأ حالات متقطعة من سوء الأداء والتوقف الشامل نتيجة الحرارة. وحتى بدون الحرارة الزائدة فإن درجة الحرارة المتغيرة داخل غلاف الحاسوب يسبب احياناً بتمددات وانكماشات تؤدي إلى ارتخاء نقاط اتصال الرقائق بشكل يكفي لتوليد عوارض غريبة. ويستحسن التأكد دائماً من ارتكاز الرقائق بشكل جيد في مقابسها. وتأكد من تفريغ جسدك من

الكهرباء الساكنة الممكن تواجدها وذلك بلمس غلاف الآلة أو أية نقطة تأريض آخر وذلك قبل لمس سطح الرقيقة.

قد تندهش لعدد الأشياء التي قد تنفك داخل الحاسوب ولكن لا يتطلب الأمر مهارة فنية لإزالة الغلاف والتأكد من ارتكاز الرقائق في مقابسها ومن سلامة التوصيلات المقبسية. ويجدر بي أن أقول بأنه لا يتطلب الأمر مهارة خاصة لفتح الحاسوب الشخصي نوع IBM أو ما يوافقه لفحص التوصيلات، ولكن غلاف الماكنتوش يشكل تحدياً أكثر صعوبة. فقد صمم خصيصاً لجعل الدخول إليه صعباً وذلك لتخفيض احتمال العبث بالنظام.

وهنالك مجموعات من مستعملي حواسيب الماكنتوش التي شكلت في العديد من المناطق في الولايات المتحدة والتي تعطي دروساً تمهيدية لمالكي حواسيب الماكنتوش الجدد والتي تشتمل على ملاحظات تساعد على فتح الآلة. ولقد حضرت مثل هذه الدروس التي كانت تعطيها المجموعة BMUG في باركلي في ولاية كاليفورنيا وهي أكبر مجموعة في العالم لمستعملي الماكنتوش. وقد ادهشني مشاهدة كيف أن أدوات فتح الغلاف التي يستعملونها والمصنوعة من مفاصل الأبواب القديمة المتوفرة في المنزل، تجعل مهمة فتح غلاف الماكنتوش الصعبة والمرهقة مسألة سهلة. ولا يجب أن يصل بك الأمر إلى حد محاولة فتح الغلاف بالخلع إلاّ إذا كنت تملك مفك البراغي الخاص نوع Trox الضروري لإزالة براغي الغلاف بما فيها اللولبين المختبأين تحت المسكة واللولب المختبىء في حجرة البطارية.

حقيقة فيروسية

إحدى أهم مقتنياتك بعد حصول عدوى فيروسية هي النسخ المساندة للفات معطياتك وبرامجك والتي يجب الاحتفاظ بها في مكان مختلف مع جعلها محمية ضد الكتابة. وكذلك يجب الاحتفاظ بنسختين مساندتين ومحميتين ضد الكتابة لبرنامج نظام التشغيل.

وحالما تصبح داخل الماكنتوش أو الحاسوب الشخصي وبمساعدة دليل جيد فإنه من الممكن حتى للمبتدىء الذي يعمل بحذر وتؤدة من تتبع بعض أسباب سوء الأداء. وإثنان من أفضل الكتب الدليلية لهذا العمل هي الدليل **Chilton's Guide to Macintosh Repair and Maintenance** تأليف Gene W. Williams لحواسيب الماكنتوش و **SAMS IBM PC Troubleshooting and Repair Guide** تأليف Robert C. Brenner للحواسيب الشخصية. وهنالك أيضاً دليل Chilton لسلسلة حواسيب الأبل والحواسيب الشخصية IBM و Kaypro وغيرها من الحواسيب الصغيرة.

وقد تكون أقراص التشخيص والتصليح وسائل مساعدة مهمة وبمساعدتها ومساعدة الأدلة

تستطيع حل معظم هذه المشاكل. وتملك بعض الحواسيب أيضاً إجراءات للاختبار الذاتي كجزء من نظام تشغيلها. وتعمل هذه عادة تلقائياً عند تشغيل الحاسوب.

ويمكن تصليح العديد من مشاكل الاحماء الزائد بمجرد معاينة محيط عمل الحاسوب واتخاذ الإجراءات التي تخفض من الحمل الحراري. تأكد من انسياب الهواء بحرية حول الحاسوب وفيه ومنه ومن عدم وجود مصباح أو أشعة شمس أو سخان أو غيرها من مصادر الحرارة تؤدي إلى إنشاء مشكلة في التبريد أو تفاقمها. واحياناً يكون استعمال مروحة لزيادة انسياب الهواء حول النظام هو كل ما تحتاجه.

هل الثلاجة أو السخان الكهربائي أو الغسالة أو مكيف الهواء موصولة على نفس الخط الكهربائي الذي يتصل به حاسوبك؟ هل الكبلات ملفوفة معاً بشكل مرتب؟ هل يوجد سجادة مريحة على الأرض؟

يجب أن تأخذ جميع هذه الأمور بعين الاعتبار إذا كان حاسوبك يتصرف بغرابة، بما في ذلك إعطاء خرج مشوش يرتبط عادة بنشاط فيروسي أو علل برامجية. وإذا كشف أحد البرامج التشخيصية عدم وجود عطل في العتاد فإن المشكلة لا يكون بالضرورة في العتاد بل مع النوعية المختلفة للطاقة الداخلة فيها. و«الطاقة القذرة» أو الطاقة التي تتغير بشكل يتجاوز مدى الفولتية العادي أو التي تحتوي على تشويش قد تكون سيئة قبل الأقراص المتسخة. ويجب تشغيل كل نظام باستعمال جهاز للوقاية ضد التمور (Surge protector) لعزله عن التراوحات الكبيرة في امداد الطاقة.

والارتفاعات الحادة للفولتية المتزايدة أو الانقطاع في التيار عند هبوط الفولتية، أو الاندفاعات الفجائية (التمورات) في الكهرباء الساكنة، أو الصواعق بإمكانها جميعاً الإضرار بالمعطيات أو التسبب بحالات سوء أداء غريبة. وتدعى هذه التنويعات والتشويشات الكهرومغنطيسية احياناً بـ **التشويشات الضجيجية أو الحالات العابرة للطاقة** وقد تنتج عن عدة تأثيرات. قد لا تستطيع شركة الكهرباء المحافظة على امداد نظيف وكاف من الكهرباء بالقرب من موقع عملك، وحتى ولو استطاعت ذلك فإن التشويشات الضجيجية قد تنتج عن الأجهزة داخل المبنى غير الموصولة بالضرورة مع نفس خط الكهرباء. والاسلاك المارة بالقرب من بعضها البعض بإمكانها نقل التشويشات الضجيجية ما بين بعضها البعض. ومجرد لف أحد الأسلاك يؤدي إلى توليد أنواع مختلفة من المجالات غير المتوقعة من الطاقة الكهربائية والمغنطيسية التي قد تؤثر على نظامك تأثيراً سيئاً.

وتحريك إحدى الأجهزة المساعدة مثل الطابعة قد يؤدي فجأة إلى المشاكل بسبب التقاط

الحاسوب لتشويش صادر عنها. وتحريك النظام قد يضعه في منطقة مليئة بالغبار أو التشويش إضافة إلى إمكانية تسبب هذا العمل إلى إرخاء إحدى الرقائق أو ازعاج سواقة الأقراص أو جعل إحدى التوصيلات غير محكمة التوصيل. افحص التوصيلات دائماً إذا كان هنالك حالة سوء أداء وتأكد دائماً من أحكام شد اللوالب التي تمسك بالقوابس في مقابسها.

وإحدى الطرق البسيطة والجاهزة لفحص التشويش هو تحريك جهاز راديو صغير ونقال بالقرب من الحاسوب والاستماع إليه لمعرفة عما إذا كان يلتقط تشويشاً بإمكانه التأثير على معالجة المعطيات. وتحتاج إلى توليف الراديو إلى محطة ضعيفة ومحاولة عدة موجات.

وقد تتعرض فجأة إلى مشكلة عندما تتغير الرطوبة أو يحرك الكبل. وقد تكون أنت السبب في المشكلة نتيجة سيرك على سجادة من الصوف بثياب مصنوعة من البوليستر أو القطن مما يؤدي إلى تراكم كهرباء ساكنة في جسمك ومن ثم تسليط 10000 فولت من الكهرباء في نظامك عندما تلمسه.

وأسباب وعوارض سوء أداء الحاسوب نتيجة المصادر الكهربائية كثيرة وعديدة. ولا حاجة إلى معرفتها طالما تتذكر بأن الطاقة القذرة والضجيج يجب اعتبارها إحدى مسببات التصرف الغريب لنظام الحوسبة.

علل البراجيات

إحدى أكثر تصرفات الحوسبة غرابة على الاطلاق باستثناء تلك التي تسببها هجومات الفيروسات أو الديدان هي نتيجة علل البراجيات.

ولا تستطيع حتى الشركات المصنعة الرئيسية إنتاج توليفات من البراجيات والعتاد الكاملة. مثلاً وفي أوائل العام 1990 أتلفت بعض طرازات الحاسوب IBM PS/2 الملفات خلال تشغيلها البرنامج Windows/386 من شركة Microsoft. وقد ظن بعض الضحايا بأنهم عرضة لهجوم فيروسي ولكن الواقع أظهر بأن المشكلة كان سببها إيعازات غامضة في البرنامج والتي تطلبت تصحيحاً في العتاد وفي البراجيات.

وكما الحال مع الفيروسات فإن علل البراجيات قد تؤدي إلى عدة مشاكل مزعجة مثل تجميد لوحة المفاتيح وتحويل كل ما هو على الشاشة إلى معلومات عديمة المعنى ومحو المعطيات وغيرها. وإذا أردت معرفة المزيد عن العلل اقرأ الكتاب **The Frozen Keyboard, Living with Bad Software** إعداد Boris Beizer وهو كتاب مليء بالمعلومات ومسلي تنشره الدار TAB Professional Reference Books.

وللتخفيف من مشاكل علل البرامجيات إلى أقصى حد لا تستعمل سوى البرامـج المشهورة والتي اثبتت جدارتها. وإذا توقفت عن العمل أو تصرفت بغرابة استشر أولاً دليل البرنامـج والملفات في الملف README على الأقراص الأصلية. وإذا لم تعط هذه الحلول المرجوة فاستشر وكيلك.

تحتاج احياناً إلى تحمل العلل فـي برامجك المفيدة جداً والتي لا تستطيـع العمل من دونها. ويصبـح العمل اسهل إذا ما حاولت التأقلم مـع خاصيات ونقاط ضعف البرامجيات الحساسة مثلما تفعل عندما تغير ناقل السرعة قبل الأوان بقليل من سيارتك القديمة التي يدور محركها بسرعة أعلى من اللزوم عند الوضعية الثانية، أو كما تعتاد على طريقة العمل الخاصة الغريبة لمحمصة الخبز الكهربائية القديمة. واحد الأساليب الذي ينفـع دائماً هو عدم جعل ملفاتك تصبـح كبيرة جداً فهي تؤدي إلى حصول العلل التي تسبب بعسر هضم للمعطيات!

حقيقة فيروسية

البرنامـج الخدماتي الذي يدّعي القدرة على تصليح الضرر الفيروسي واستعادة الملفات «المفقودة» قد يكون خطيراً في حال استعماله استعمالاً غير صحيـح. تأكد من قراءة الأدلة التي ترفق مـع تلك البرامـج.

ومـع علل البرامجيات وحالات سوء الأداء العتادي، فإن التشخيص يعني القيام بعملية بطيئة ومنهجية لمراجعة جميـع الأمور التي قد تخطيء، والأعمال الواجب القيام بها عند بروز المشكلة، وجميـع التغييرات التي تمت على النظام قبل أن يبدأ النظام بالتعطل. والمحافظة على دفتر يوميات للمعطيات قد يساعد كثيراً على الوصول إلى قلب المشكلة. وتسجيل أعمال الحوسبة قد يفيد من عدة نواحي فهو يساعد على تحديد مدى الضعف حيال عدوى الفيروس والمناطق حيث يجب اتخاذ إجراءات وقائية، وتوفير معلومات تساعد على عملية التعافي.

تقوم الحواسيب بمعالجة المعلومات ولكن العديد من الأنظمة لا تولد معلومات كافية حول الطريقة التي يجري فيها استعمالها. والاحتفاظ بدفتر يوميات للحوسبة هو طريقة فعالة لملء هذه الفجوة في المعلومات. واليوميات النموذجية المبينة لاحقاً يمكن استعمالها كبداية. واليوميات التي تحمل شعار الأقراص هي لتسجيل نشاطات البرامجيات، وتلك التي تحمل صورة الحاسوب ولوحة المفاتيـح هي للمعلومات التي تتعلق بالعتاد.

واعمل على تصوير أو مراجعة صفحات السجل الأسبوعي في نظامك واستعمالها كما هي أو تعديلها لتتلاءم مـع حاجاتك المعينة. قد تفضل على سبيل المثال دمجها في صفحة سجل واحدة أو إضافة الأعمدة لمعلومات خاصة. ويمكنك تغيير العناوين بحيث تتوافق دفاتر اليومية للحواسيب مـع أعمال حفظ السجلات الأخرى التي تتبعها.

وعند استعمال دفاتر يوميات المعطيات كأدوات إدارية شخصية أو أعمالية فإنك تكتسب أيضاً معلومات قد تساعدك على جعل أعمالك الحاسوبية أكثر فعالية من ناحية الكلفة. وحتى بعد أسبوع أو أسبوعين يتكون لديك فكرة عن مدى استعمال البرامج التطبيقية المختلفة وما هي الخدمات المتصلة بالخط التي تستعمل كثيراً ومدى استعمال ووثوقية العتاد وغيرها من المعلومات المهمة.

وهذا النوع من المعلومات يمكن استعماله بعدة طرق. مثلاً، حالما تحدد التطبيقات والمعطيات المستعملة كثيراً تستطيع تنظيم القرص الصلب بحيث يتم الوصول إلى تلك البنود بسرعة. وقد تلاحظ أيضاً انماط تتطور قد تشير إلى الأسلوب الأفضل الواجب اتخاذه عند إعداد إجراءات لحماية المعطيات.

وإذا كنت مسؤولاً عن إدارة عملية للحاسوب اطلب من كل مشغل أن يحضر مثل هذه الدفاتر اليومية وذلك لغرض استعمال أساليب حوسبة آمنة. والمعلومات المستخلصة من هذه الدفاتر اليومية تنشيء أيضاً صورة تبين مدى فعالية استعمال العتاد والبراجيات وتوفر دليلاً يساعد على التخطيط لشبكات الحواسيب وجدولة مواعيد استعمال المرافق مثل الطابعات وإجراء عمليات شراء أو استبدال.

6 ما العمل عند وجود الفيروس

المعلومات الموجودة في هذا الفصل هي عبارة عن مرجع سريع يتعلق بجميع النقاط الرئيسية لفيروسات الحاسوب التي قد تحتاج الاضطلاع عليها. واعتبر هذا القسم من الكتاب وكأنه قاعدة معطيات عشوائية الوصول. وتصور نفسك تستعمل ازرار الهاتف الإلكتروني للوصول مباشرة إلى المعلومات التي تحتاجها لتخفيض خطر التعرض للعدوى إلى أقصى حد، أو لتشخيص وعلاج الهجوم الفيروسي.

القائمة الرئيسية المبينة على الصفحة التالية هي دليلك للوصول إلى المعلومات الموجودة في هذا الفصل. وهي تشبه قوائم الخيارات التي تجدها في العديد من برامج الحاسوب السهلة الاستخدام. ولكي تجد المعلومات التي تريدها اختر رقم انتقاء من 1 إلى 5 ثم انتقل مباشرة إلى العنوان المناظر في هذا الفصل. وبإمكانك أيضاً تصفح هذه الشجرة من معلومات فيروس الحواسيب كيفما تريد أيضاً. وتستطيع دراسة قاعدة المعطيات هذه بالتتابع الذي تريده ولكنك سوف تجد المعلومات في كل قسم مرتبة بتتابع تدريجي من القرارات والأفعال التي يجب أن تتخذها على شكل المخطط البياني لسياق العمل (flow chart).

وتستطيع صنع نسخ من هذه الصفحات ووضعها على لوحة الملاحظات الجدارية أو في حافظة أوراق في موقع عملك بحيث تتمكن من الوصول إليها مباشرة في حال حصول طارىء ما. وإذا كنت مسؤولاً عن أمن المعطيات وحمايتها في مؤسسة ما تتواجد فيها عدة مراكز عمل تستطيع وضع نسخة عن تلك الصفحات عند كل لوحة مفاتيح.

القائمة الرئيسية

1 ـ النجدة!
اعتقد أني التقطت عدوى فيروسية. ماذا أفعل؟
2 ـ موجز
موجز عن الفيروس
3 ـ التشخيص
كيف تحدد أنواع الفيروس الرئيسية
4 ـ الاستعادة
ملاحظات تساعد على التخلص من عدوى الفيروس
5 ـ الوقاية
كيف تخفف خطر التعرض لعدوى الفيروس بنسبة 95 بالمئة.

1 ـ النجدة! أعتقد أني التقطت عدوى فيروسية. ماذا أفعل؟

لا تجزع وحافظ على رباطة جأشك فقد يكون إنذار خاطىء. والآن إتبع الخطوات التالية:

1 ـ إفصل الطاقة عن حاسوبك إلا إذا وجب عليك حفظ عملك الحالي. فالوضع لا يستطيع التفاقم إذا توقف حاسوبك عن العمل، أو قم بحفظ عملك على أقراص إذا استطعت وأوقف الحاسوب.

2 ـ ضع جميع الأقراص التي استعملتها خلال جلسة العمل هذه في ظرف والصق عليه بطاقة واكتب عليها «أقراص مصابة بعدوى فيروسية».

3 ـ وطالما لا تزال ذاكرتك قوية أكتب وصفاً قصيراً للعوارض التي جعلتك تشك باحتمال وجود عدوى فيروسية. وأجب بعد ذلك على الأسئلة التالية. وإذا كان هنالك جواب إيجابي فحاول تزويد أكبر قدر من التفاصيل الممكنة. قد لا تستطيع الإجابة على بعض تلك الأسئلة الآن ولكن سوف نتطرق إليها لاحقاً.

هل استغرق تلقيم البرامج وقتاً أكثر من المعتاد؟

نعم ☐ كلا ☐

تفاصيل:

هل استغرقت عمليات الوصول الأخرى للأقراص وقتاً أكثر من المعتاد؟

نعم ☐ كلا ☐

تفاصيل:

هل حصلت نشاطات غير عادية على الشاشة؟

نعم ☐ كلا ☐

تفاصيل:

هل حصلت حالات سوء أداء للعتاد؟

نعم ☐ كلا ☐

تفاصيل:

هل اختفت بعض الملفات؟

نعم ☐ كلا ☐

تفاصيل:

هل ظهرت ملفات غريبة؟

نعم ☐ كلا ☐

تفاصيل:

هل ظهرت رسائل تحذيرية؟

نعم ☐ كلا ☐

تفاصيل:

هل اشتغلت مصابيح السواقات بدون سبب؟

نعم ☐ كلا ☐

تفاصيل:

هل انخفضت فسحة التخزين المتوفرة على القرص؟

نعم ☐ كلا ☐

تفاصيل:

هل حصلت زيادات في حجم البرنامج؟

نعم ☐ كلا ☐

تفاصيل:

هل تغيرت أحجام الملفات القابلة للتنفيذ؟

نعم ☐ كلا ☐

تفاصيل:

4 ـ أسرد أسماء الملفات التي وصلت إليها عبر الشبكة أو الهاتوف (modem)، واية أقراص غريبة استعملتها في النظام، وأسماء الأشخاص الذين استعملوا النظام مؤخراً، والأقراص التي استعملتها على نظام آخر ثم استعملتها في نظامك، وأية ظروف ممكن أن تكون قد أدت إلى حصول فيروس.

الأقراص المستعملة:

حالات الوصول إلى الشبكة:

المستعملون المختلفون:

5 ـ إتصل بمدير نظام المعلومات الإدارية (MIS) أو المسؤول عن الشبكة أو أحد المستشارين أو صديق متمرس في الحواسيب، أو بالجهة التي تتصل بها عادةً عند حصول طارىء في عملية معالجة المعطيات أو أحد المصادر الأخرى ذات الخبرة في الحواسيب. واكتب اسم ورقم هاتف ذلك الشخص هنا الآن:

إشرح للخبير العوارض المسردة في الخطوة 4 واتبع النصيحة أو التعليمات التي تتلقاها.

وقد تكون وحيداً في هذا الوضع الطارىء لعملية معالجة المعطيات ولا تستطيع الحصول على مساعدة. ولديك في هذه الحالة خيارين:

- انتظر حتى تتوفر مساعدة من خبير. وهذا يجب أن يكون خيارك الأول إلاّ إذا كنت واثقاً جداً من قدراتك أو إذا كنت سوف تتعرض لخسارة كبيرة إذا ما فقدت المعطيات المخزونة في القرص الصلب.
- تابع العمل في لائحة الفحوصات هذه وحاول تحديد الفيروس وازالته بنفسك إذا كان هنالك من فيروس. وقبل إتخاذ قرار إعادة وصل الطاقة ومتابعة العمل اعتبر النقاط التالية:

ـ هل المعلومات المجمعة في الخطوة 4 تشير إلى أن احتمال وجود عدوى فيروسية هو الاحتمال الأكبر؟ هل تأكدت من عدم وجود مشاكل في العتاد أو علل في البراجيات (راجع الفصل الخامس).

ـ وحتى ولو كان هنالك فيروساً في النظام فقد لا يكون قد أثر على معطيات مهمة. هل تستطيع المجازفة بخسارة تلك المعطيات إذا ما ارتكبت خطأً ما عند محاولة استئصال الفيروس؟

ـ هل تستطيع المجازفة بخسارة المعطيات والبرامج التطبيقية لأنك تملك نسخاً مساندة جيدة لها؟

ـ هل تملك برنامج فعال لتشخيص الفيروس و/أو اكتشافه، أو هل تستطيع الحصول على مثل هذا البرنامج.

ـ هل تملك خبرة كافية في الحوسبة بحيث تتمكن من متابعة العمل دون مساعدة خبير وبالتالي المخاطرة بخسارة المزيد من المعطيات أكثر مما قد أتلف حتى الآن؟

إذا قررت المتابعة فاتبع الخطوات التالية. وقبل البدء ضع الكتاب الدليلي المرفق مع برنامجك التطبيقي بالقرب منك، فسوف تحتاج إليه لمقارنة التفاصيل الأصلية للبرامج مثل الحجم والعنوان وحقوق الطبع وغيرها، مع ما يحصل على المرقاب لمعرفة التغييرات التي أجراها الفيروس.

6 ـ إعزل نظامك عن توصيلات الشبكة. وانتبه إلى أن فصل الخط المؤدي إلى الشبكة بشكل خاطىء قد يسبب ببعض المشاكل في بعض الأنظمة.

تذكر بأنه من المحتمل أن تكون قد تعرضت لفيروس بقطاع الاستنهاض والذي يعمل لحظة وصل النظام بالطاقة. ولهذا تحتاج إلى تركيب النظام DOS عن مصدر نظيف مثل الأقراص الأصلية والتي تكون محمية ضد الكتابة بواسطة العروات اللاصقة الخاصة بالحماية ضد الكتابة. ولا يصلح في هذه الحالة سوى الحماية المادية ضد الكتابة فوسم تلك الملفات على أنها مقروءة فقط لا يحميها ضد البرامج الفيروسية. وإذا كنت تستعمل أقراصاً حجم $3\frac{1}{2}$ إنش فقم بتحريك الفرضة إلى وضعية الحماية. واتبع الخطوات التالية لتركيب النظام DOS:

7 ـ إذا كنت تملك سواقة للأقراص المرنة ضع نسخة محمية ضد الكتابة لأقراص النظام DOS الأصلية في السواقة A. وبوضع قرص DOS نظيف في السواقة A تتجاوز التلقيم التلقائي للنظام DOS من القرص الصلب الذي قد يكون ملوثاً. وإذا كنت لا تملك سوى سواقات للأقراص الصلبة فإن أية فيروسات في قطاع الاستنهاض يجب أن تكون قد حجزت في الظرف العازل الذي استعملته سابقاً.

8 ـ أوصل الحاسوب بالطاقة واستنهض حاسوبك مراقباً أي نشاط غير عادي. سوف يبدأ النظام DOS بفحص نظامك عارضاً عنواناً وحقوق الطبع وغيرها من التفاصيل ومن ثم يعرض الوقت والتاريخ حاثاً إياك على إدخالها من جديد. وإذا حصل نشاط غير هذا فقد يشير ذلك إلى عدوى فيروسية.

الخطوة التالية هي لأولئك الذين يملكون برنامجاً مضاداً للفيروس مثل ViruScan. وإذا لم تكن تملك برنامجاً فعالاً مضاداً للفيروسات أو مصدر استشاري خبير انتقل إلى الخطوة «3. التشخيص ـ كيف تحدد أنواع الفيروس الرئيسية» وابحث عن العوارض المسردة آنفاً ثم عد إلى الخطوة 10 في هذا القسم. مثلاً سوف تراقب لتتأكد عما إذا كانت شاشات العنوان وحقوق الطبع للبرنامج التطبيقي عادية وأن حجم البرنامج (عدد البايتات المسردة) مماثل لمواصفات الناشر. إذا كان الحجم أكبر مما يجب أن يكون عليه فإن هذا دليل لاحتمال وجود فيروس.

9 ــ يشغل البرنامج المضاد للفيروس واتبع تعليماته بحذر. توضع مثل هذه البرامج عادة على قرص مرن محمي ضد الكتابة لوقايته من الفيروس.

SCAN C:

إذا وجد البرنامج المضاد للفيروس عدوى في قطاع الاستنهاض (أو إذا أشارت العوارض إلى ذلك) حاول التخلص منه باستعمال الأمر SYS. عندما تستعمل هذا الأمر فإنك تستبدل البرنامج DOS الملوث على القرص الصلب ببرنامج DOS النظيف الموجود على القرص غير الملوث في السواقة A.

10 ــ أدخل الأمر **SYS C:** عند المحث A > . وإذا تم تحويل النظام دون مشاكل فسوف تحصل على الرسالة.

system transferred

كرر هذه العملية مع جميع الأقراص المرنة الاستنهاضية الملوثة لأنها تحتوي على أوامر نظامية للنظام DOS. ويستحسن مساندة المعطيات فقط والتخلص من الأقراص المشتبه بها. وإذا أخفق الأمر SYS بإزالة عدوى قطاع الاستنهاض ولا تزال تريد متابعة العمل بمفردك فحاول مساندة جميع ملفات المعطيات قبل تنفيذ الخطوة التالية التي تعيد نسق القرص الصلب.

11 ــ ولإعادة نسق القرص الصلب راجع دليل النظام DOS واتبع الإجراءات المذكورة هناك بحذر.

قد تكون عملية إعادة نسق القرص الصلب ومن ثم إعادة تركيب جميع ملفات المعطيات من النسخ المساندة، والبرامج التطبيقية من أقراصها الأصلية، عملية صعبة جداً ومزعجة نفسياً. ولكن البديل قد يكون أسوأ بكثير في حال لم يتم إزالة عدوى الفيروس بالكامل بحيث تعود لاحقاً لتسبيب المزيد من الأضرار. ولا تستطيع الوثوق بالقرص الصلب سوى عن طريق إعادة النسق واتخاذ التدابير الاحترازية المناسبة خلال إعادة تركيب ملفاتك. وكخلاصة، إذا تعرض حاسوبك للعدوى ولا تعرف شيئاً عن موضوع الفيروسات لا تتأخر باستشارة خبير إذا لاحظت إحدى العلاقات التالية عن عدوى الفيروس:

- عمليات تلقيم البرامج والوصول إلى الأقراص تستغرق وقتاً طويلاً.
- فسحة التخزين في الذاكرة والقرص انخفضت فجأة.
- ظهور رسائل أخطاء أو شاشات عرض غير عادية.
- ملفات تختفي و/ أو ملفات غريبة تظهر.
- تغييرات تحصل على حجم الملفات القابلة للتنفيذ.
- مصابيح السواقات تعمل بدون سبب.

وعمل مهم جداً آخر للطوارىء يجب القيام به عند التعرض لعدوى فيروسي هو الاتصال بجميع من قد يتعرض لنفس الفيروس وتحذيره، كالأشخاص الذين اتصلت بهم مؤخراً عبر الشبكة أو تبادلت معهم الأقراص. وبهذه الطريقة تستطيع منعهم من خسارة معطياتهم وقد يستطيعون مساعدتك إذا ما كانت تواجههم نفس المشاكل.

2 ـ موجز عن الفيروس

فيروسات الحواسيب هي مجرد برامج حاسوبية أو أقساماً من شيفرة ذاتية التناسخ. وتلصق الفيروسات نفسها مع البرامج وقد تبقى مختبأة حتى يحين الوقت الذي ضبطت عنده لتعمل. ويقوم البعض منها بإتلاف أو تغيير ملفات المعطيات والبرامج الأخرى. والبعض منها من النوع المازح وبعضها غير ضار. ولكن البعض الآخر قد يؤدي إلى كوارث. فقد تقوم على سبيل المثال بمحو جميع ما يوجد على القرص الصلب. وبعض الفيروسات توقف النظام كلياً وذلك بالتوالد إلى حد يستهلك الذاكرة بأكملها. والفيروسات لا تضر بعتاد الحاسوب إلا في حالات نادرة.

كيف تنتشر الفيروسات

بإمكان فيروسات الحواسيب التكاثر والانتشار من حاسوب إلى آخر بواسطة الأقراص الملوثة أو وصلات شبكة الحواسيب أو البرامج الملقمة من لوح الإعلان الحاسوبي. واستلام قرص مرن من صديق أو السماح لمندوب مبيعات من استعمال نظامك هي الطرق المعتادة التي يدخل فيها الفيروس إلى النظام. ولا يعرف عادةً الشخص الذي يملك القرص الملوث بأنه يحتوي على فيروس ولهذا فإن الكثير من الفيروسات تنتشر عن غير قصد من قبل الأصدقاء وزبائن العمل.

وباستطاعة الفيروسات التنقل بسرعة من محطة عمل إلى محطة أخرى عبر الشبكات المناطقية المحلية (LAN) لتصل إلى ملقم الملفات المناطقي المحلي (file server). وهي تنتشر عبر ألواح الإعلان الحاسوبية حيث تختبىء الشيفرة الملوثة داخل براجيات عامة أو تشاركية مثل البرامج التطبيقية المفيدة أو الألعاب الحاسوبية المسلية التي لا تقوى على مقاومة إغراء تلقيمها.

ويمكن من الناحية النظرية عمل جميع أوساط الاتصال الإلكترونية كمسار لانتشار الفيروسات وذلك بين الآلات في نفس الغرفة أو عند الجانب الآخر للعالم.

أنواع الفيروس الرئيسية

هنالك ثلاثة أنواع رئيسية من الفيروسات. الفيروسات الملوثة لقطاع الاستنهاض التي تلصق نفسها بقطاع استنهاض القرص الصلب أو الأقراص المرنة التي تحتوي تعليمات بدء

التشغيل الأولي للحاسوب. وهذه الفيروسات تكتب فوق تعليمات قطاع الاستنهاض الأصلية بحيث تستلم زمام الأمور مباشرة. وهي تميل إلى إنشاء قطاعات سيئة على القرص حيث تخزن بقية شيفرة برنامجها.

وهنالك الفيروسات الملوثة للنظام التي تلصق نفسها بأجزاء مختلفة من نظام التشغيل أو برنامج التحكم الرئيسي للحاسوب. وقد يلوث الفيروس قسم الدخل/الخرج في شيفرة نظام التشغيل، أو مفسر الأوامر أو أي ملف نظامي آخر. وملوثات النظام قد تصبح مقيمة في الذاكرة لتبقى في الحاسوب مستلمة زمام الأمور طوال الوقت، أو قد تنفذ عملها القذر ثم تتلف نفسها. وهي مشكلة خاصة لأنها تتحكم بالنظام قبل أن يتمكن برنامج لإكتشاف الفيروسات أو للوقاية منها من الدخول إلى الذاكرة وأداء عمله.

وتستطيع الفيروسات الملوثة للتطبيقات العامة الأغراض التأثير على جميع البرامج التطبيقية مثل معالج الكلمات وبرنامج الصفحات المجدولة وقاعدة المعطيات أو البرامج الخاصة الأغراض وحتى تلك التي تصممها بنفسك. وهذه البرامج قد تقيم أو لا تقيم في الذاكرة وقد تقوم بالتلويث كلما لقم برنامج أو نسخ أحد البرامج من قرص إلى آخر، أو أحياناً عند الوصول إلى دليل ملفات لقرص معين يحتوي على برامج أخرى. وملوثات البرامج التطبيقية العامة الأغراض سهلة التكاثر نظراً لوجود الكثير من المناطق حيث تستطيع الاستضافة.

3 ـ التشخيص ـ كيف تحدد أنواع الفيروس الرئيسية

هنالك الكثير من المشاكل التي قد تحصل في الحاسوب ولكن معظمها يعود عادةً إلى علل برامجية أو حالات سوء أداء للعتاد. ولكن عند ظهور عارضين أو أكثر تشبه عوارض الفيروسات المشاكسة بنفس الوقت فإن احتمال وجود عدوى يزيد وعندها يجب أن تفحص نظامك بواسطة برنامج مضاد للفيروس.

وهذه بعض العوارض التي تظهر عادةً:

1 ـ تلقيم البرامج يستغرق وقتاً أكثر من المعتاد.

بإمكان بعض الفيروسات التحكم بإجراءات بدء التشغيل الأولي لنظام أو برنامج. وعند استنهاض الحاسوب أو تلقيم برنامج تطبيقي فإن هذه الفيروسات تبدأ عملها مما قد يمدد الوقت المطلوب لإتمام العمل بعدة ثواني.

2 ـ عمليات الوصول إلى الأقراص تستغرق وقتاً طويلاً لا تحتاجه مثل هذه المهمات البسيطة.

مثلاً حفظ صفحة من النص تستغرق عادةً حوالي ثانية ولكن الفيروس يمدد ذلك إلى ثانيتين أو ثلاثة. وانتبه بالأخص إلى التباطيء في عمليات الوصول إلى أدلة الملفات وإجراءات التحديث.

3 ــ ظهور رسائل خطأ غير مألوفة.

قد تصادفك الرسالة التالية:

Write protect error on drive A التي تشير إلى أن فيروساً في نظامك يحاول الوصول إلى قرص لتلويثه. وظهور هذه الرسائل يجب أن يحثك على التقصي عن العدوى الفيروسية خاصة إذا ما ظهرت الرسائل بشكل متكرر.

4 ــ مصابيح السواقات تضيء بدون سبب ظاهر.

إذا واصل أحد مصابيح السواقات على التوميض عندما لا تحاول الوصول إليها بهدف تلقيم أو حفظ المعطيات فإنك تكون على الأرجح ضحية فيروس.

5 ــ انخفاض ذاكرة النظام.

تستهلك بعض الفيروسات قدراً كبيراً من الذاكرة. وإذا كنت تقوم بتشغيل أحد البرامج الكبيرة بدون مشاكل لتفاجأ بعرض رسالة تقول بعدم وجود ذاكرة كافية في النظام فإن هذا قد يشير إلى وجود عدوى فيروسية.

6 ــ الملفات تختفي (أو تظهر) بشكل غامض.

تحذف بعض الفيروسات الملفات إما عشوائياً أو وفق تعليمات محددة. وإذا اختفى أحد الملفات من دليل ملفات بدون سبب ظاهر فيجب الشك بالفيروس. وكذلك إفحص للكشف عن الفيروس في حال ظهور ملفات لا مبرر لوجودها.

7 ــ فسحة التخزين المتوفرة على القرص انخفضت بدون سبب ظاهر.

وهذه علامة تحذيرية متكررة تشير إلى دخول الفيروس وابتدائه بالتناسخ.

8 ــ البرامج التنفيذية يتغير حجمها.

تبقى هذه البرامج عادة بنفس الحجم ولكن إذا كان هنالك عدوى فيروسية قد تتضخم وقد يزداد على الأرجح عدد البايتات المسرود. وهنالك بعض الفيروسات الذكية التي تزيد من حجم البرامج ولكنها تعيد العدد المحدد في المواصفات الأصلية.

9 ــ الإيقونات يتغير مظهرها.

إن إجراء تغييرات طفيفة في إيقونات الماكنتوش المألوفة هو أحد الأمور المحببة لصانعي

الفيروسات. وقد تظهر عوارض مماثلة في الأنظمة الأخرى التي تستعمل وسائل تداخل تعتمد الرسوم البيانية.

وحالات سوء أداء العتاد والعلل في البرامج قد تسبب أيضاً بعوارض شبيهة بالفيروس ولذا تجعل التشخيص صعباً. راجع القسم «1. النجدة ـ اعتقد أني التقطت عدوى فيروسية. ماذا أفعل؟» في هذا الفصل وما سجلته من نشاطات الحوسبة السابقة لتحدد عما إذا كنت قد تعرضت للعدوى. وإذا كانت فرصة تعرضك للفيروس ضئيلة فانتقل إلى الفصل الخامس للحصول على التفاصيل حول العلل وحالات سوء الأداء المشابهة لعمل الفيروس.

4 ـ الاستعادة ـ ملاحظات تساعد على التخلص من عدوى الفيروس

إزالة عدوى الفيروس قد يكون صعباً وإذا لم تكن ضليعاً بما يكفي بعمل الحواسيب فلا يجب محاولة ذلك دون مساعدة خبير.

والخطوات الواجب اتخاذها تعتمد على نوع الفيروس. إذا كنت تعتقد بأنك تعرضت للعدوى ولكنك لا تعرف نوع الفيروس في نظامك، راجع القسم «3 ـ التشخيص ـ كيف تحدد أنواع الفيروس الرئيسية» لمساعدتك على التشخيص أو إلى القسم «2 ـ موجز ـ موجز عن الفيروسات» للحصول على أوصاف الأنواع الرئيسية للفيروسات.

إزالة فيروسات قطاع الاستنهاض

إزالة فيروسات قطاع الاستنهاض قد تكون صعبة جداً. والأفضل الحصول على المساعدة، وإذا تعذر ذلك فاتبع هذه التعليمات بحذر.

تذكر بأن فيروس قطاع الاستنهاض يلصق نفسه بالتعليمات الموجودة في قطاع القرص والتي تلقم في الذاكرة مباشرة عند وصل النظام بالطاقة. ولإزالة هذا النوع من الفيروسات يجب أن تعكس عملية العدوى طارداً الفيروس ومعيداً تركيب شيفرة قطاع الاستنهاض الأصلية. وللقيام بذلك استعمل الأمر الخدماتي SYS للنظام DOS واتبع التعليمات المذكورة في دليل النظام DOS وتلك المذكورة في الخطوة 10 للقسم «1 ـ النجدة! أعتقد أني التقطت عدوى فيروسية. ماذا أفعل؟».

قد لا يزيل الأمر SYS دائماً فيروس قطاع الاستنهاض ولذا تحتاج إلى استعمال برنامج مصمم خصيصاً لهذه المهمة والتي تتوفر كبرامج عامة على ألواح الإعلان الحاسوبية. وأحد تلك البرامج هو MDISK والذي يمكن تلقيمه من لوح إعلان الجمعية الصناعية لفيروس الحواسيب (CVIA).

إزالة فيروسات نظام التشغيل

تلوث فيروسات نظام التشغيل برنامج واحد أو أكثر داخل نظام التشغيل ولذا يجب أن تحدد في البداية الملفات الملوثة.

1 ـ افصل الطاقة عن حاسوبك. وعندما تعيد وصله بالطاقة مجدداً استنهض النظام باستعمال القرص المرن الأصلي لنظام التشغيل المحمي ضد الكتابة.

2 ـ ولتحديد الملف أو الملفات الملوثة شغل برنامج فعال كاشف للفيروسات مثل ViruScan.

3 ـ وحالما تحدد الملفات الملوثة استعمل القرص المرن الأصلي لنظام التشغيل المحمي ضد الكتابة وانسخ النسخة الأصلية للملفات الأصلية من القرص المرن إلى القرص الصلب وذلك لإزالة شيفرة الفيروس بالكتابة فوقها.

تأكد من بقاء الأقراص الأصلية محمية دائماً ضد الكتابة ومن النسخ من القرص المرن إلى القرص الصلب وليس بالعكس.

إزالة فيروسات البرامج التطبيقية

تؤثر فيروسات البرامج التطبيقية على جميع أنواع البرامج التطبيقية. اتبع الخطوات التالية للتخلص من هذه الفيروسات:

1 ـ افصل الطاقة عن النظام وعندما توصل الطاقة مجدداً إعمل على الاستنهاض من القرص المرن الأصلي المحمي ضد الكتابة لنظام التشغيل.

2 ـ استعمل برنامج خدماتي لمسح الفيروسات من أجل مسح ملفات تلك البرامج (التي تنتهي عادة باللواحق EXE. أو COM. وتحديد تلك الملوثة.

3 ـ احذف جميع هذه الملفات الملوثة من النظام باستعمال أمر الحذف DEL للنظام DOS بإدخال **DEL** ثم فراغ يليه اسم الملف الملوث.

4 ـ اجلب الأقراص والمستندات الأصلية للبرنامج التطبيقي واستعملها لتكرار إجراءات التركيب بحيث يتم استبدال الملفات الملوثة بالنسخ الأصلية غير الملوثة.

5 ـ الوقاية ـ كيف تخفض خطر التعرض لعدوى الفيروس بنسبة 95 بالمئة

هنالك أربعة طرق رئيسية لتخفيض خطر التعرض للتلوث بالفيروس إلى أقصى حد:

1 ــ استعمل البرامج الخدماتية الكاشفة وبرامج مسح الفيروس التي تحدد وجود العدوى.

2 ــ استعمل برامج منع العدوى لتحقيق حد أدنى على الأقل من الوقاية ضد الفيروس الذي اخترق النظام.

3 ــ استعمل البرامج الخدماتية للتعريف والإزالة من أجل تحديد نوع الفيروس الذي سبب الفيروس ولمساعدتك على إزالته.

4 ــ اتبع «القواعد الذهبية العشرة للحوسبة الآمنة» المذكورة عند نهاية هذا القسم.

وتعمل برامج الاكتشاف بإحدى طريقتين. النوع الأول ينشيء «لقطة» للنظام مسجلاً تفاصيل معينة مثل أحجام قطاع الاستنهاض، وملفات نظام التشغيل، وجميع البرامج التنفيذية. وتخزن هذه المعلومات في ملف سجل على أنها «لقطة أو المقياس الذي يحدد النظام النظيف. وعند تشغيل المرحلة الثانية من هذا النوع من برامج الاكتشاف فإنها تفحص الحالة الراهنة للنظام بمقارنتها مع المقياس الموجود في ملف السجل وإذا ظهر اختلاف فقد يكون هنالك فيروس. مثلاً قد تتضخم بعض الملفات بسبب التصاق شيفرة فيروسية بها. أما النوع الثاني من برامج الاكتشاف فتسمى ببرامج اللقاح. وبرامج اللقاح تدخل فعلياً في برامجك التطبيقية وتجري فحصاً ذاتياً بحيث كلما استعملت برامج معالجة الكلمات أو الصفحات المجدولة على سبيل المثال، يجري فحصها بحثاً عن أي عدوى محتملة. وتعرض رسالة في حال اكتشاف الفيروس.

تعمل برامج منع العدوى بمراقبة نظامك للانتباه إلى أي عمل يشير إلى وجود برامج فيروسية. مثلاً تلصق معظم الفيروسات نفسها مع أقسام أخرى من النظام مثل قطاعات الاستنهاض على القرص بهدف التناسخ. ويحفز النوع المرشحي من البرامج المضادة للفيروسات عندما تكتشف نشاط يتميز به الفيروسات. مثلاً، قد يوقف أحد تلك البرامج الفيروس عن الوصول إلى ملف تنفيذي. ويعرض رسالة تحذيرية على المرقاب.

والبرامج المضادة للفيروسات العاملة على التعريف والإزالة تخفض الخطر إلى أقصى حد عن طريق التعرف أولاً على النشاط الفيروسي المميز ومن ثم إزالة الشيفرة المسؤولة عن ذلك النشاط. وتقوم هذه البرامج بمسح النظام برمته باحثة عن الفيروسات. وإذا وجدت إحداها تظهر رسالة تحذيرية على الشاشة تعرّف عن نوع الفيروس ومكان وجوده في النظام ومبيد التلوث المعين المطلوب. وبالطبع ونظراً للإنشاء المستمر لفيروسات جديدة وتعديل الفيروسات الموجودة فإن هذه الفيروسات قد لا تصلح دائماً ضد الضغوطات الجديدة التي تتنكر بشكل جيد وفعال.

يقدم القسم التالي القواعد الذهبية العشرة للحوسبة الآمنة. وإذا تقيدت بها فسوف تحمي نفسك ضد معظم المخاطر التي قد تلوث نظامك.

القواعد الذهبية العشرة للحوسبة الآمنة

1 ــ لا تقم ابداً بتلقيم أقراص غير معروفة في نظامك أو السماح لأي كان القيام بذلك إلّا بعد التأكد من خلوها من الفيروسات.

2 ــ لا تستعمل أقراصك في نظام آخر إلّا بعد وضع عروة الحماية ضد الكتابة.

3 ــ لا تقبل البرامج إلا بعد التأكد من خلوها من الفيروسات. وحاول إبقاء البرامج والمعطيات على أقراص مستقلة.

4 ــ انتبه كثيراً عند استئجار الحواسيب أو استعمال مراكز النشر المكتبي التي لا تتبع إجراءات احترازية مشددة مضادة للفيروسات.

5 ــ إذا توجب تبادل الأقراص أو تشغيل البرامج أو المعطيات على أنظمة غريبة اتبع إجراءات عزل فعالة. لا تقم على سبيل المثال بتشغيل أقراص قد تكون ملوثة على النظام الرئيسي وخاصة إذا كان مزوداً بقرص صلب. أعمل على فحصها أولاً على نظام معزول وغير أساسي مثل الحاسوب النقال غير المزود بقرص صلب، أو مع قرص مرن في السواقة الثانية. إذا كنت تشغل برامجك ومعطياتك الخاصة على أنظمة غريبة انسخها أولاً إلى أقراص مساندة واستعمل هذه الأجهزة في النظام الآخر واتلفها عند الأنتهاء من العمل. لا تأخذ تلك الأقراص معك مجازفاً بتلقيمها دون قصد لاحقاً في نظامك الموجود في المنزل أو المكتب.

6 ــ لا تلقم البرامج من ألواح الإعلان الحاسوبية أو من شبكة حواسيب لا تتمتع بإدارة جيدة أو لا تعتمد إجراءات ضد الفيروس. وإذا اقتضى الأمر إسأل مشغل النظام عن الإجراءات المضادة للفيروس المتبعة.

7 ــ لا تسمح لأحد باستعمال حاسوبك بمفرده ودون مراقبة وخاصة عند احتمال وضعه لأقراصه في نظامك. تذكر بأن العدوى بإمكانها الانتشار على يد اعز أصدقائك.

8 ــ انتبه إلى أية تغيرات لا مبرر لها بطريقة عمل نظامك مثل اشتغال السواقة بدون سبب ظاهر.

9 ــ استعمل عروات الحماية ضد الكتابة وانشىء وسوماً للأقراص تسجل حجم برامجك.

وكلما شغلت البرامج افحص الوسوم بانتظام لاكتشاف أي نشاط غريب قد يشير إلى حصول تناسخ فيروسي.

10 ـ للحماية ضد خسارة المعطيات لأي سبب كان إعمل على مساندة المعطيات بانتظام على أقراص لا تحتوي على شيفرة برامج. ازل التلوث من جميع أوساط التخزين ولا تستعمل أقراص المساندة دون التأكد أولاً من أنها ليست ملوثة أيضاً. و 90 بالمئة تقريباً من جميع المؤسسات التي تعاني من الفيروس تتعرض بعد شهر مجدداً إلى العدوى، إما بسبب أقراص مساندة ملوثة أو لأنها لم تنظف أنظمتها جيداً.

7 وقاية المعطيات ومنع عدوى الفيروس

والآن ننتقل إلى الأخبار السارة! يعيد إليك هذا الفصل سلطة التحكم على حاسوبك التي يحاول مهووسو الحواسيب واشقياء الفيروس انتزاعها منك.

ويمكنك في الواقع تخفيض احتمال تعرضك لعدوى الفيروس بنسبة 90 بالمئة والجيد في الأمر هو أنه رغم تعرضك للعدوى فإنك تملك القدرة على التعافي بدون ألم مع تخفيض الضرر إلى أقصى حد.

والخبر السار الأهم هو قدرتك على المحافظة على أكثر أجزاء نظامك أهمية وهي المعطيات عند حصول الكوارث الطبيعية وغير الطبيعية التي قد تصادفها. ويشمل هذا الأمر علل البرامج وحالات سوء أداء العتاد إضافة إلى الهجومات الفيروسية.

وتصرف عادة الكثير من المال على العتاد الذي يشكل الآلية المحسوسة الجالسة على منضدك. وتصرف أيضاً على الأرجح نفس القدر من المال وربما أكثر على البرامج التطبيقية التي تحول العتاد إلى أدوات مفيدة.

ولكن سرعان ما يضمحل هذا الاستثمار المالي بالمقارنة مع قيمة المعطيات التي يتيح لك العتاد والبراجيات جمعها. وهذه المعطيات فريدة. والعتاد والبراجيات يمكن تبديلها بسهولة وقد تكون كلفة تبديلها في حال حصول كوارث حاسوبية زهيدة إذا تجاهلنا الأزعاج المترتب عن ذلك، وخاصة إذا كانت معداتك مضمونة لدى شركة تأمين.

ولكن لا يوجد مخزن أو شركة تستطيع توفير بديل لمعطياتك التي هي ثمرة تعبك وجهدك. وحماية معطياتك التي تشكل أهم موجودات الحوسبة لديك وأكثرها قيمة، هو من مسؤوليتك وحدك. ولحسن الحظ فإن ذلك ليس صعباً ولا يتطلب خبرة فنية خاصة ولا يكلف كثيراً.

ويجب من الناحية المثالية شمل كل نظام حاسوب ضمن خطة طوارىء تغطي معظم الكوارث المحتملة. وسوف نتطرق إلى تفاصيل تلك الخطة في الفصل العاشر. وربما أنت تملك

إجراءات احترازية واهتمامك الحالي ينحصر بمنع عدوى الفيروس، ولذلك فإن هذا الفصل يركز على وقاية معطياتك. وكفائدة إضافية، فإن تخفيض إمكانية التعرض إلى الفيروسات وعواقبها إلى أقصى حد بإمكانه أن يزيل تلقائياً معظم المخاطر الأخرى التي تسبب بفقدان المعطيات.

استعمل وسائل الحماية المادية لوقاية النظام

واللغط الفني الذي تولده الحوسبة بشكل عام والفيروسات بشكل خاص يحجب احياناً الحقيقة الأساسية التي تشير إلى أن الفيروس هو مشكلة أشخاص. القاعدة الأولى للوقاية من الفيروس هو حماية نظامك من الأشخاص الذين قد يعرضونه للعدوى عن قصد أو غير قصد.

يعرض الأشخاص سيارتك للأذى بنفس الطريقة، فعندما تكون واقفة لا تتحرك قد يلحق بها أشخاص آخرون الضرر عن طريق خلعها عمداً أو بالاصطدام بها دون قصد أو حرمانك منها كلياً بسرقتها. وإذا كنت قلقاً حيال حصول هذه الأمور تقوم بقفل سيارتك ومحاولة ركنها في مواقع قليلة الخطر. وتنتبه بالأخص إلى عدم وضع أشياء ذات قيمة داخلها أو بوضعها في أماكن مخفية مثل صندوق السيارة.

وينطبق نفس الأمر على حاسوبك، فخط الدفاع الأول لنظام الحاسوب وللمعطيات الموجودة فيه يتألف من وسائل الحماية المادية التي تتخذها لحمايتها من التفاعل الضار مع الأشخاص. حدد اولئك الأشخاص بعناية فخطرك الأكبر قد يصدر من أعز أصدقائك أو أكثر موظفيك ثقة أو حتى أحد أفراد عائلتك. وكذلك اعتبر مسألة حماية أقراصك مسألة مقدسة فهي المصدر الأساسي لعدوى الفيروس.

احصر الوصول إلى النظام

يشكل جميع من يستطيع الوصول إلى نظامك إما مادياً أو إلكترونياً عبر وصلة هاتف أو شبكة حواسيب أو بإعطائك الأقراص، خطراً محتملاً. حدد جميع الطرق التي قد تنتقل فيها العدوى واتخذ التدابير الاحترازية المناسبة. حاول الدخول إلى نظامك بنفسك كاشفاً نقاط ضعفه. وإذا كنت مسؤولاً عن نظام حاسوب لشركة فحاول تنظيم عملية اقتحام. ولقد استفادت الكثير من الشركات وتعلمت الكثير عن جميع نواحي أمن حواسيبها باستعمال «فرق النمور» (Tiger Teams) المعدة على شكل وحدات عسكرية والتي تحاول غزو أنظمتها.

وحصر الوصول قد يقتصر على وضع النظام في مكتب مقفل أو غرفة مقفولة أو خزانة

مقفلة حسب الوضع المعين. ولا يمكن إصابة نظامك بالعدوى اطلاقاً أو تعرض معطياته للتلف إلّا إذا سنحت لأحدهم الفرصة لتشغيل برنامج ملوث.

والأمن المادي يجب أن يمتد إلى جميع الأقراص أو أوساط التخزين الأخرى مثل أشرطة التسجيل أو القرص الصلب النقال. وإذا لم يكن من العملي وضع النظام بأكمله في مكان مقفل فهنالك ملحقات عتادية متوفرة تمنع قيام أي شخص بتشغيل الحاسوب، وهنالك أيضاً براجميات تمنع حصول استعمال غير مسموح عن طريق كلمات المرور. ولكن تذكر بأن بعض اسوأ الفيروسات تبدأ العمل لحظة استنهاض الحاسوب ولذا فحتى أكثر أنظمة كلمات المرور تطوراً قد لا يمنع قرصاً ملوثاً من إدخال الفيروس إلى نظامك.

لا تسمح باستعمال النظام سوى لأولئك الذين يحتاجون لاستعماله فقط وذلك مع مراقبة مشددة للحرص على اتباع أساليب الحوسبة الآمنة في جميع الأوقات. والسماح بالوصول غير المحصور للحاسوب يزيد من خطر دخول العدوى. ولقد قام الحاسوب الشخصي أو الحاسوب النقال في المنزل حيث يستعمله جميع أفراد العائلة مثلما يستعملون الفرن الكهربائي أو جهاز الفيديو، بنقل الفيروسات المنتشرة في المدارس والجامعات إلى أنظمة الشركات.

وقد ينسى الأولاد تحذيراتك في يوم من الأيام ويضعون في الحاسوب الشخصي الموجود في المنزل قرصاً يحتوي على لعبة حاسوبية أو فرض منزلي التقط العدوى من نظام المدرسة أو النظام في منزل أحد الأصدقاء. وينتقل الفيروس مباشرة إلى القرص الصلب أو إلى قرص في سواقة أخرى أو يبقى منتظراً في الذاكرة RAM. وقد يستعمل هذه الحاسوب الشخصي المنزلي احياناً للأعمال، ولكن لا يحتاج سوى إلى مرة واحدة لينتقل الفيروس إلى قرص يحمل من المنزل إلى المكتب. وهذا القرص الذي يوضع لاحقاً في نظام متصل بشبكة يستطيع التأثير على المئات وربما الآلاف من حواسيب الشركة قبل ظهور أية عوارض. ويمكن في الواقع أن يبرمج الفيروس بحيث يبقى مختبئاً إلى حين وصوله إلى شبكة شركة. ويجري تفعيله هناك عبر تلميحات مثل اسماء بعض الشركات المعينة التي تظهر في مستندات معالج الكلمات أو الصفحات المجدولة للمحاسبة.

والشركات الواعية تقوم بتشجيع موظفيها على ممارسة أساليب الحوسبة الآمنة في أنظمة منازلهم مثلما يفعلون مع الوسائل المتطورة المتوفرة في منازلهم. ويعتبر بعضها الأنظمة المنزلية لموظفيهم كبوابات لأنظمة الشركة والتي يجب حمايتها مثلما تحمى تلك الموجودة في الشركة.

وتعرض نظامك للعدوى أيضاً عندما تسمح لمندوبي بيع البراجميات أو المستشارين أو غيرهم من الغرباء بالوصول إلى حاسوبك لتشغيل البرامج الإعلانية أو للقيام بمهام أخرى.

وإذا لم يكن بإمكانك منع مثل هذا الوصول المادي إلى النظام فاعمل على حصره بأكبر قدر ممكن على الأقل، وإذا لم تستطع تجنب ذلك اطلاقاً فاجعل هؤلاء الغرباء يسلمون أقراصهم للمعاينة قبل وضعها في النظام. ما تريده هو تجنب أي خطر «للعنف الإلكتروني» في محيط حوسبتك، فالفيروس يشبه المسدس المحشو الذي قد ينطلق إما عمداً أو خطأ.

وقد يكون حصر الوصول المادي بشكل قاسي على الموظفين صعب في بعض حالات العمل. والموظفون الذين لا يحتاجون فعلاً إلى استعمال الحاسوب لوظائف عملهم لا يجب السماح لهم باستعمالها. وغالباً ما تكون جلسات اللعب الحاسوبية خلال فترة الغداء وكذلك مصدر التلويث الجديد (بأكثر من طريقة) لمحيط عمل المكتب المتمثل بالعاب الحاسوب الخلاعية، مصادر لحصول عدوى الفيروس.

تذكر بأن جميع الموظفين الذين يستطيعون الوصول إلى نظام حساس يستطيعون أيضاً تخريب ذلك النظام إذا ما ارادوا ذلك. والعديد من الشركات تقوم بسرعة بعزل الموظفين المطرودين فوراً عن نظام الحاسوب. ولكن تذكر بأنه إلى حين اتخاذ هذا العمل قد يكون قد وضع فيروس ضار في النظام. ويستحسن فحص النظام بحثاً عن الفيروس في جميع الحالات التي قد تتعرض فيها الشركة للانتقام كما قد يحصل خلال الاضرابات أو الاختلافات النقابية.

والاحتفاظ بسجل مكتوب عن نشاط الحاسوب يؤكد للموظفين ضرورة الأمن وقد يعطي نتائج مهمة في حال حصول عدوى. ولكن السجل أو دفتر اليوميات بمفرده (كتلك المذكورة في الفصل الخامس للعتاد والبراجيات) لن يحمي ضد الوصول غير المخوّل. ويمكن توسيع إجراءات تسجيل الدخول والخروج التي تحضر للأنظمة بحيث تسجل نشاط البرامج التطبيقية في النظام. وقد تكون هذه الإجراءات على شكل ملف دفعي بسيط. وتحوي مجلة PC Magazine بعض الأمثلة على تلك الملفات في إحدى فقراتها تحت عنوان PC Magazine bulletine board. ولا تخزن مثل هذه السجلات إلكترونياً (في الحاسوب) فقط لأنها قد تفقد في حال حصول عدوى فيروسية، بل احتفظ بنسخ مطبوعة منها.

عندما قامت مجلة PC Magazine بتقييم شامل للبراجيات المضادة للفيروس في أحد مقالاتها الرئيسية، قامت باختبارها على فيروسات موجودة. وخلال إجراء أعمال التقييم اتخذ القائمون على الاختبار تدابير احترازية تشدد على النقطة التي اشرنا إليها سابقاً بخصوص حصر الوصول المادي والتي تنقلنا إلى اهتمامنا التالي وهو ضبط الأقراص.

«لقد طلب من القائمين على اختبار برامج الوقاية العمل وراء أبواب مغلقة في قسم خاص من مختبر الحواسيب الشخصية للمجلة وعدم السماح لأي شخص غير مخوّل من الدخول (فالأقراص المرنة تختفي فجأة عند وجود عدة أشخاص)». هذا ما كتبه المحرر المساعد دونالد ب. ويلموت.

إضافة إلى ذلك فإن جميع الأقراص التي تحتوي الفيروسات والمستعملة في الأبحاث وضعت في علبة حمراء مقفلة. ومن المهم جداً في جميع محيطات الحوسبة المحافظة على سلامة الأقراص غير الملوثة لمنع الاستعمال غير المخوّل والذي قد يؤدي إلى عدوى فيروسية.

إحم الأقراص وابعد الأقراص الغريبة

تسبب الأقراص الملوثة على الأرجح معظم حالات العدوى بالفيروس. ولا يجب تشغيل الأقراص الغريبة إلّا بعد فحصها طبعاً، ولكن الأقراص المستعملة في نظام نظيف قد تتعرض للعدوى دون أن يلاحظ أحد ذلك. فقد تؤخذ مثلاً لتستعمل في نظام آخر ضمن المكتب أو في المنزل (المسافة المقطوعة لا علاقة لها بخطر التقاط العدوى).

قد تنقل القرص إلى الطرف الآخر من الغرفة أو إلى آخر الرواق لمعالجة معطياتك على طابعة لايزرية أو راسمة مشتركة فيلتقط العدوى هناك. وقد تأخذه إلى المنزل لأنهاء المشروع خلال عطلة الأسبوع على حاسوبك الشخصي حيث قد يتعرض للعدوى من عدة مصادر. وقد تنقل القرص مسافة قصيرة على منضدتك لتعيده بعد ذلك إلى مكانه الأصلي وذلك عندما تريد تحويل المعطيات أو برنامج ما من حاسوبك العادي إلى حاسوبك النقال. وهذه الرحلة القصيرة بإمكانها أن تؤدي إلى كارثة.

لا تعر احداً أقراص برامجك اطلاقاً فقد تلتقط العدوى وتعيدها إلى نظامك. وإذا كان لديك سبباً وجيهاً لإعادة البرنامج فقم بنسخ القرص وعند إعادته لك أتلفه أو أعد نسقه.

وهذه الحالات وغيرها من حالات نقل القرص مادياً من نظامك إلى نظام آخر تخلق فرصاً لانتشار العدوى، ولكنها جميعها نظرياً مجرد ظروف تستطيع التحكم بها وفرض جميع التدابير الاحترازية المنطقية عليها. أما منع الأقراص الغريبة من دخول محيط حوسبتك إلى أن تبرهن بأنها خالية من الفيروسات قد يكون مهمة أكثر صعوبة. فهذه الأقراص الخطرة بإمكانها الدخول إلى نظامك بطرق لا تشير إلى وجود خطر اطلاقاً.

لا يجب أن تسمح لأحد من جلب أقراص برامجه لاستعمالها على نظامك. كما لا يجب قبول البرامج كهدايا أو على أساس الإعادة وبالأخص النسخ المقرصنة غير الشرعية للبرامج الامتلاكية. وقد تنقل النسخ المقرصنة عدة مرات بحيث تكون قد مرت على عدة أنظمة قبل وصولها إليك، والتي قد يكون إحداها ملوث.

واحذر بالأخص وكلاء المبيع الذين يحاولون إغراؤك بتلقيم القرص الصلب على حاسوبك الجديد أو تزويدك بأقراص مرنة تحتوي على مجموعة من البراامجيات «المجانية». وقد تكون تلك المجموعة نوعاً من البرامجيات العامة أو البرامجيات المشتركة الخاضعة لحقوق طبع

التي لا يطلب منـك سوى الارتباط اخلاقياً برخصة الناشر ودفـع قيمة مالية صغيرة إذا ما قررت استعمالها، أو قد تكون نسخة مقرصنة لبرنامـج تجاري امتلاكي منسوخة دون اذن. وبغض النظر عن مصدر هذه البرامـج فيجب الاشتباه والشك بها لناحية خطر التعرض للفيروس.

> **حقيقة فيروسية**
>
> تستطيـع بعض البرامـج الخدماتية فحص حالة البرامـج والأقراص بسهولة كبيرة. ويستحسن استعمال هذه البرامـج بانتظام وبالتالي إنشاء روتين حوسبة آمن يعطي مردوداً كبيراً.

وتذهب الشركات الحذرة وبعض مستعملي الحواسيب العاديين إلى حد إخضاع أقراص البراجميات الامتلاكية الأصلية الموضبة إلى فحوصات للفيروس أو إلى نوع من الخطر الصحي قبل استعمالها. وهذه التدابير الاحترازية قد أصبحت ضرورية بسبب العدوى المتعمدة أو العرضية التي تحصل في البراجميات التجارية وحتى في بعض الأصناف المشهورة.

ويقوم بعض موزعي البراجميات بزيادة عدد ضحايا الفيروس دون أن يدركوا ذلك بسبب سياسة التبادل ورد البضاعة التي يتبعوها. إذا اشتريت برنامجاً ولم يعجبك أو وجدت عيباً فيه فإن العديد من الشركات تسمـح لك بإرجاعه لقاء تبديله أو إعادة ثمنه. وهذه السياسة كانت في البداية في مصلحة المستهلك إلى أن بدأ وباء الفيروس بحيث أصبحت تخلق الفرص لدخول الفيروسات إما عمداً أو عن غير قصد في البراجميات المعادة. والرزمة المعادة والملوثة قد تباع إلى زبون آخر، ولذا لا تشتري ابداً برنامـج غير موجود في رزمته الأصلية المختومة. ولكن حتى هذا الأمر ليس بضمانة أكيدة بأن البراجميات التي اشتريتها خالية من الفيروسات وذلك لأن بعض الشركات تعيد ترزيم الأقراص المعادة وبيعها وتوزيعها من جديد. ويؤمل بأن ينخفض أسلوب العمل هذا على الأقل بالنسبة لناشري البراجميات المسؤولين الذين يريدون حماية شهرتهم. وقد أصبـح هذا الأمر غير مرغوب مثل إعادة بيـع الثياب الداخلية أو فراشي الأسنان المستعملة!!

استحصل دائماً وحيثما أمكن وبالتوافق مـع احتياجاتك على آخر إصدار للبـرنامـج المعروف. فالناشر المشهور للبراجميات يواصل دائماً تحسين منتوجاته بحيث يجب أن تحتوي الطبعة 3 للإصدار 2 (التي يشار إليها عادة بالرمز 2.3) على عدد أقل من العلل غير المرغوبة من الإصدارات السابقة.

وسوف تواصل الفيروسات تلويث البراجميات الامتلاكية ولكن الناشرين الرئيسين يتخذون الآن تدابير احترازية معقدة لتقليل الخطر إلى أقصى حد بحيث يكون أقل من خطر البرامـج المقرصنة أو البراجميـات المشتركة أو البراجميات العامة على الأقل. وتعرف شركـات تصنيـع

البراجيات بأنها قد تتعرض لشتى أنواع الملاحقات القضائية إذا ما ادعى أحدهم بأنها نشرت الفيروسات في براجها الأصلية الموضبة. ولكن لا تتوقع رؤية بطاقات تشير إلى أن الرزمة «خالية من الفيروس» حتى على المنتوجات التي هي نظيفة بشكل شبه مؤكد.

بعض أساليب الوقاية ضد الفيروس

إذا ما شغلت قرصاً غريباً قد يكون ملوثاً وبالأخص قرصاً يحتوي برنامجاً جديداً، ولا تملك برنامجاً فعالاً لإكتشاف الفيروس حاول أولاً على الأقل فتحه كملفات معطيات قرائية في معالج كلمات. عاين الملفات باحثاً عن رسائل غير مألوفة أو وقحة ضمن إيعازات برمجة غير مفهومة. وبعض الفيروسات تتميز برسائل معينة وقد ترغب بصرف الوقت بحثاً عن كلمات دليلية مثل «warrning» أو «virus» أو «ha-ha» إلى جانب الكلمات البذيئة المعتادة. تحقق من اسم وعنوان ورسالة حقوق الطبع للمؤلف أو الناشر. وإذا لم تكن موجودة أو تبدو زائفة فيجب الشك بوجود عمل تخريبي. ولكن احذر: فحص البرمجة عن طريق تمريرها في معالج كلمات قد يكون كافي لإطلاق بعض أنواع الفيروسات كاحتمال بعيد.

والإجراء الاحترازي الآخر هو قراءة المستندات الموجودة على القرص التي ترفق مع البرنامج الجديد والموجودة عادةً في ملفات تحمل اللاحقة TXT . أو DOC .. وبرنامج جيد التصميم من نوع حصان طراودة يعمل على نشر الفيروس قد يحتوي على ملف README ليزيد من خداعه والإيهام بأنه قسم بريء من البراجيات، ولكن إذا كانت التعابير أو النوعية الأدبية للنص في ذلك الملف ضعيفة فيجب اعتبار هذا تحذيراً بوجوب عدم تشغيل البرنامج.

عروات الحماية ضد الكتابة هي واقيات رائعة للأقراص ويجب أن تستعملها دائماً على أي قرص لن يحتاج إلى كتابة المعطيات عليه وهذا يشمل أقراص البرامج والأقراص التي تخزن عليها الأرشيف والنسخ المساندة. ولصق العروة اللاصقة على حزوز الأقراص المرنة حجم $5\frac{1}{4}$ إنش أو تحريك العروة على الغلاف البلاستيكي للأقراص المرنة حجم $3\ \frac{1}{2}$ إنش يعزلها عن أي هجوم فيروسي لاحق. وإذا كان القرص ملوثاً أصلاً فإن حمايته ضد الكتابة يشبه إلى حد بعيد قفل باب الإسطبل بعد انطلاق الحصان ولكنك تعلم على الأقل بأن هنالك فيروس محتمل في نظامك: إذا حصلت على رسالة خطأ غير مبررة تتعلق بالحماية ضد الكتابة عند وجود قرص محمي في السواقة رغم أنك لا تحاول الوصول إليه فاعتبر هذا تحذيراً بوجود عدوى فيروسية محتملة.

إعمل دائماً على حماية قرص الاستنهاض لنظام التشغيل ضد الكتابة ولا تستعمل سوى ذلك القرص لاستنهاض النظام المزود بسواقتين للأقراص المرنة فقط. أما إذا كنت تملك قرصاً

صلباً يحتوي على نظام التشغيل تستطيع بمساعدة دليل النظام DOS توسيع نطاق الحماية أكثر بجعل الملفات COM . و EXE . محمية ضد الكتابة بحيث تصبح من النوع القرائي فقط (Read-only). وهذا الإجراء يختلف في إصدارات النظام DOS المختلفة، وهنالك برامج خدماتية متوفرة لتسهيل هذا العمل.

إذا كنت تملك قرصاً صلباً لا تقم أبداً بتشغيل الحاسوب مع وجود أقراص مرنة في السواقات. وهذا لضمان الاستنهاض من القرص الصلب دائماً وليس من إحدى السواقات التي قد تحتوي على قرص صلب بفيروس لقطاع الاستنهاض يتولى استلام زمام أمور النظام فوراً.

ويستحسن القيام دورياً باستبدال ملفات نظام التشغيل المعرضة للتلوث في القرص الصلب بتلك الموجودة على قرص نظام التشغيل الأصلي الذي تعرف بأنه خال من الفيروس. وإضافة إلى الملفات COM . و EXE . و SYS . التي تشكل الأهداف المفضلة للفيروسات لا تنسى مسيقات الفأرة ومسيقات الأجهزة الأخرى التي تلقم من الملف CONFIG. SYS واعمل على استبدالها بانتظام أيضاً.

يجب الحذر الشديد عند استعمال ألواح الإعلان الحاسوبية

بسبب وظيفتها الأساسية كوسط اتصال لتبادل المعطيات وشيفرة البرمجة أيضاً فإن ألواح الإعلان الحاسوبية، معرضة كثيراً لتتحول إلى ناقلات للفيروس. ولكن ألواح الإعلان الفيروسية مهمة جداً كمرفق خدماتي إلى حد لا يسمح بتجاهلها ولكن شرط إتخاذ تدابير احترازية مثل اختبار ملفات البرامج قبل تلقيمها.

رغم محاولة العناصر الضارة على ألواح الإعلان الحاسوبية إغراؤك لا تلقم أي برنامج من ألواح الإعلان الحاسوبية المشكوك بها في حاسوبك. وابتعد عن الألواح التي توزع البرامجيات المقرصنة فإن احتمال تعرضك لفيروس حاسوبي مماثل لالتقاطك فيروس بشري عند ارتيادك لمقهى أو مسبح غير نظيف.

وهنالك عدد متزايد من المستعملين الذين يجدون متعة وفائدة في التجوال داخل ألواح الإعلان الحاسوبية يفعلون ذلك على حاسوب مخصص لذلك الغرض. وإذا حصل والتقطت فيروساً وحددته تستطيع عزله في ذلك النظام وعدم نقله إلى نظامك الرئيسي حيث قد يلوث ملفات المعطيات. وهذا استعمال جيد لنظام قديم أصبح بطيئاً أو محدود القدرات بالنسبة لاحتياجات الحوسبة الرئيسية، أو لحاسوبك الثاني إذا كنت تملك حاسوباً عادياً وحاسوباً نقالاً. والأفضل عدم احتواء الحاسوب الثاني على قرص صلب حيث قد يستطيع الفيروس الاختباء

ما بين جلسات العمل مع ألواح الإعلان الحاسوبية بانتظار الفرصة للخروج من مخبأه والبحث عن ضحايا جدد.

وتلقيم البرامج التي تم ضغطها لتوفير المكان على ذاكرة اللوح ووقت الإرسال على الخط قد أصبح مشكلة خاصة. فعملية الإنضغاط وإزالة الإنضغاط تتطلب برامج خاصة ولهذا فإن هذه البرامج هي أمكنة جيدة يمكن فيها إخفاء الفيروسات وجعل الفيروسات تتحفز للقيام بالأضرار التي شرحناها سابقاً.

إذا قمت بتلقيم برنامج ما مباشرة على القرص الصلب من لوح إعلان حاسوبي أو من شبكة حواسيب أو نظام للبريد الإلكتروني أو غيرها من المصادر فقم على الأقل بوضعه في مكان منعزل مؤقت قبل تشغيله والمخاطرة بإطلاق الفيروس بين المعطيات والبرامج على القرص الصلب.

والطريقة للقيام بذلك هي بنسخ الملف الملقم أولاً على قرص مرن فارغ منسق حديثاً ولا يحتوي على أي شيء وخاصة على ملفات لنظام التشغيل. واحذف بعد ذلك من القرص الصلب الملف الذي لقمته ولا تستعمل البرنامج الجديد إلا بعد اختباره من القرص المرن وعلى نظام معزول إذا أمكن بقرص صلب لا يحتوي على معطيات مهمة قد يلحق الضرر بها. ولا يجب تلقيم البرنامج الجديد في القرص الصلب إلا بعد اجتيازه الفحص الطبي. وإذا كان هنالك أدنى شك تخلص من القرص الذي يحتوي على البرنامج فلا جدوى من المخاطرة.

وإحدى الأمور الأساسية للاحتفاظ بزمام أمور نظامك هي امتلاك أسلوب التفكير الصحيح. فتجميع البرامج لأنها جذابة أو رخيصة وتكديس الأقراص لأنك لا تعتبرها أشياءاً يجب رميها هو أسلوب تفكير خطر. فالأقراص كلفتها زهيدة عند مقارنتها بالمعطيات ولذا لا تتردد بإتلافها إذا ما كانت ملوثة.

وبعض البرامج المتوفرة على ألواح الإعلان الحاسوبية أو المباعة في لقاءات هواة الحواسيب تبدو وكأنها تقدم مزايا لا غنى عنها ولكن كما الحال مع جميع الصفقات فهنالك شرك. والبرنامج الجيد سرعان ما يشتهر ولن يختار مؤلفه بدون شك بأن يظل غير معروف. ولهذا فإن البرنامج غير المعروف الذي لم يرفقه المؤلف باسم موثوق يجب أن يكون موضع شك. وكذلك الأمر بالنسبة لبرنامج صغير الحجم يدّعي بأنه يعطي نتائج كبيرة ومتطورة. وهذه التلميحات يجب أن تجعلك تشك بأن البرنامج الذي لقمته من اللوح أو حصلت عليه على قرص قد يحتوي على فيروس مختبأ في حصان طروادة. وفي هذه الحالة فإن العمل الوقائي الأفضل هو حذف ذلك البرنامج من القرص الصلب أو إعادة نسق القرص المرن الذي خزّن عليه وعدم المجازفة أكثر من ذلك.

استعمل براجيات مضادة للفيروس حديثة وجيدة النوعية

قد تعتقد بأن هذا يجب أن يكون الأمر الأول على لائحة إجراءات الوقاية ضد الفيروس ولكن في الواقع فإن البراجيات المضادة للفيروس هي سيف ذو حدين وقد تكون أحياناً خطيرة جداً.

وبعض البرامج المضادة للفيروس لا تنفع إطلاقاً. وقد وجد المقاولون في جميع أنحاء العالم في وباء الفيروس فرصة ذهبية لجني المال السريع فقاموا بعرض براجيات مضادة للفيروس عديمة النفع والمسؤولية. وبعض البراجيات غير فعالة لأنها أنزلت إلى الأسواق بسرعة دون اخضاعها لعملية تطوير واختبار جيدة، بينما البعض الآخر غير قادر على توفير الوقاية التي تعلن عنها.

وبعض البراجيات قد يكون فعالاً لفترة من الوقت ولكن في حال عدم مواصلة تحديثه يصبح عديم النفع في منع العدوى بالنسبة لعدد كبير من الفيروسات الجديدة التي تواصل الظهور.

وعند كتابة هذا الكتاب لم يكن هنالك بعد معيار قياسي لتقييم البراجيات المضادة للفيروس أو جمعية حكومية أو جمعية للمستهلكين لوضع قواعد لهذا التقييم. ويواجه حتى خبراء الحواسيب صعوبة في الحكم على فعالية المنتوجات المختلفة عند عدم امتلاكهم لمعرفة مختصه بالفيروسات، وتظهر بعض المقالات المهمة المنشورة جهلاً وبساطة يثيران العجب.

وفي العام 1989 قام إثنان من أهم الأسماء الموثوق بها في عالم الحواسيب هما شركة IBM و Apple بإصدار رزم لبراجيات مضادة للفيروسات فعالة نسبياً ولكنها لم تزود وقاية شاملة. وقد كتبت هذه البرامج بشكل جيد واختبرت بمسؤولية ووفرت إجراءات وقاية واستعادة فعالة ضد فيروسات معينة. ولكن إذا كنت تملك أحد هذه البرامج لحاسوب الماكنتوش أو الحاسوب الشخصي خاصتك فلا تستطيع الاعتماد عليها لحمايتك كلياً نظراً لكتابة فيروسات جديدة طوال الوقت تهدف إلى التغلب على جميع البراجيات المضادة للفيروسات. وأحد البرامج الجيدة المضادة للفيروسات هو البرنامج ViruScan الذي تم اختباره في ظروف متعددة من قبل عدة شركات لديها الخبرة الضرورية لإصدار أحكام ذات قيمة. واضافة إلى ذلك يمكن تحديث ViruScan بسهولة. وهنالك برامج أخرى متوفرة تستحق نفس التقدير ولا يستطيع أي كتاب التكلم عنها والنصح باستعمالها لفترة طويلة.

الأسلوب الأفضل هو تتبع ملاحظات الإعلام المسؤول والأخبار المتعلقة بوباء الفيروس واستعمال إصدارات جديدة لبراجيات مضادة للفيروس موصى بها من مصادر مشهورة.

ولا تعتمد على تقارير المنتوجات الجديدة في المجلات التي تضع إعلانات للشركات المصنعة لهذه المنتوجات قبل اختبار تلك المنتوجات. ويقوم جميع ناشري البراجميات المضادة للفيروسات تقريباً كما يفعل مصنعو حبوب الصداع بالإدعاء بإن منتوجهم يشفي كلياً. ولا ينطبق هذا على أي برنامج مضاد للفيروس وهنالك القليل فقط ممن يقترب من تنفيذ وعودهم الظاهرة.

وتشكل جميع هذه البرامج في حال جعلتك تعتقد بأنك في أمان خطراً أكبر من عدم استعمالها إطلاقاً. وإذا كنت تعتمد كلياً عليها وتعتقد بأنك لا تحتاج إلى إتباع مباديء الحوسبة الآمنة الأساسية التي حددت في هذا الفصل فإنك تكون قد وضعت ثقتك في ما يشبه إلكترونياً زيت الأفاعي.

هنالك أربعة أنواع أساسية من البراجميات المضادة للفيروسات تستطيع الاختيار منها. وسوف نتناول خصائصها المميزة ونسلط الضوء على بعض نقاط ضعفها المبيتة.

منتوجات الوقاية هي مثل بوابات الأمن للبراجميات يراد منها منع الفيروسات من دخول النظام. وهذه المنتوجات تقوم إما بمنع النشاط غير العادي أو تحذرك بأن عملاً سيئاً يجري بحيث تقرر ما يجب عمله. وهي تعيق نشاط الفيروس العادي بالبحث عن الخصائص الإسمية لفيروس عادي وتحاول منع البرنامج الغازي حالما تشتبه بشيء ما. وهي تتصرف مثل حارس الأمن عندما يواجه دخيل يتصرف بطريقة خطرة.

وإضافة إلى دروعها الدفاعية الإسمية المضادة للفيروسات تملك بعض المنتوجات الوقائية قدرة على إطلاق الإنذار للتحذير ضد تشغيل البرامج التي لم يعط لها إذن تشغيل. وهي تشبه إجراءات التفتيش التي تتطلب من الأشخاص إبراز بطاقة هوية قبل الدخول إلى النظام. ورغم فعالية هذه البرامج فإنه يمكن للفيروسات الذكية استغفالها والاختباء في البرامج المخوّلة. ويلعب العامل البشري دوره إذا ما أعطى المنتوج إنذارات خاطئة متعددة فقد تفقد ثقتك به بحيث لا تستجيب لندائه عندما يجد سبباً وجيهاً لإطلاق الإنذار.

منتوجات الإكتشاف تعطي القليل من الوقاية ضد دخول الفيروس إلى النظام ولكنها تطلق الإنذار وقد توقف نشاط النظام العادي إذا ما وجدت عدوى. والكلمة المهمة هنا هي «إذا»، فكما الحال مع البرامج الأخرى المضادة للفيروسات فإن منتوجات الإكتشاف هي حل وسط ما بين العمل المثالي وما يمكن تحقيقه عملياً. وهي تقوم بمراقبة نظامك بحثاً عن نشاط فيروس اسمي وعن تغييرات في الطريقة المعتادة التي يعمل بها نظام التشغيل والبرامج التطبيقية. وكلما تم صنع المزيد من الضغوط الفيروسية، وكلما إزدادت الفيروسات ذكاءاً في تمويه نشاطاتها وتقليد التطبيقات المشروعة فإن كلاً من منتوجات الوقاية والإكتشاف تصبح قديمة العهد وغير فعالة.

وتصنف الفئة الثالثة من البراجيات المضادة للفيروس كمنتوجات تعريفية والتي تقوم بعد حصول العدوى بمقارنة العوارض مع عوارض الفيروسات المعروفة وتبلغك الضغوطات التي تتطابق مع تلك العوارض وتزود عادةً بعض المساعدة حول كيفية إزالة العدوى. وهذا النوع من المنتوج المضاد للفيروس قد يصبح أيضاً قديم العهد بسرعة كبيرة مثل الطبيب الذي لا يتتبع التطور العلمي في مجال الطب.

لقد أصبح من الشائع لأهداف تسويقية إضافة إلى أسباب أخرى تسمية البرامج المضادة للفيروسات باسم **منتوجات التلقيح**. وبالمعنى الطبي، يتألف اللقاح من فيروسات غير خبيثة أو جزيئات من الفيروس الميت أو فيروسات تم إضعافها والتي تولد جميعها مضادات حيوية لمحاربة نوع معين من العدوى الفيروسية. ومنتوج التلقيح للفيروس الحاسوبي لا يتصرف بنفس الطريقة وهذا الإسم يطبق عادةً على منتوجات الإكتشاف التي تطلق الإنذار إذا ما حصل تغيير في البرامج التنفيذية. وبما أن بعض هذه البرامج تفحص نفسها في أي حال فقد يحصل تعارض ما بين برنامج التلقيح والبرنامج التنفيذي الذي يسعى إلى حمايته مما يؤدي بالتالي إلى توليد إنذارات خاطئة.

وتركز بعض البراجيات المضادة للفيروس على أسلوب معين للتحكم بالوقاية أو الإكتشاف أو الضرر، بينما يجمع البعض الآخر ما بين العناصر من نوعين أو أكثر. والنوع الذي تختاره سوف يعتمد على عدة عوامل مثل مدى اهتمامك بخطر الفيروس ومدى تعرضك لهذا الخطر. وإذا اعتمدت حلاً وسطاً واخذت جميع الأمور بعين الاعتبار فإن أكثر البرامج المضادة للفيروسات وقاية سوف يقوم بمراقبة نشاط نظامك بشكل مكثف. وهذا بالتالي سوف يبطىء العمل ويزيد من احتمال حصول إنذارات خاطئة أكثر مما يقوم به برنامج مضاد للفيروسات أقل فعالية.

ولا سبب يدعو إلى اعتماد وقاية براجية تعيق الاستعمال الفعال للنظام. وإذا أدى المنتوج المضاد للفيروس إلى إبطاء العمل كثيراً أو التعارض مع برامجك التطبيقية التي تحتاج إلى استعمالها أو إصدار الكثير من الإنذارات الخاطئة فإن حالك تكون أفضل بدونه، أو على الأقل عدم استعماله كجزء منتظم لعملك الروتيني على النظام. ركّز على أساليب الحوسبة الآمنة الأساسية الأخرى فتتمكن من تخفيض خطر العدوى إلى مستوى مقبول خاصة إذا كنت تتبع سياسة مساندة فعالة للمعطيات.

وعوضاً عن أخذ جرعات زائدة من الأدوية الإلكترونية الواقية عند وقوع المشكلة أو عند الاشتباه بها، استعمل المنتوجات التعريفية المضادة للفيروسات مثل ViruScan مثلما تستعمل الاختبار الطبي وذلك فقط عند وجود ما يبررها. واحتفظ عادةً بنسختين من البرنامج ViruScan بالقرب مني جاهزة للاستعمال عند حصول طارىء.

ربما تملك وسائل لإكتشاف الفيروس واستعادة المعطيات من النوع القوي جداً ولكن ليس الكامل وذلك على شكل برنامج خدماتي يراقب نشاط النظام ويسترد الملفات «المفقودة». ولكن إحذر بإن البرنامج الخدماتي القوي قد يضر بنظامك إذا لم يستعمل بحذر. ويجب على مستعملي الحواسيب المتمرسين استعمالها بحذر أيضاً واتباع الإجراءات المذكورة في الدليل. وغالباً ما نحاول تشغيل البرامج التطبيقية دون قراءة الدليل المرفق معها قبل ذلك ومتجاهلين تلك الأدلة كلما سنحت لنا الفرصة. وهذا العمل خطير مع البرامج الخدماتية القوية.

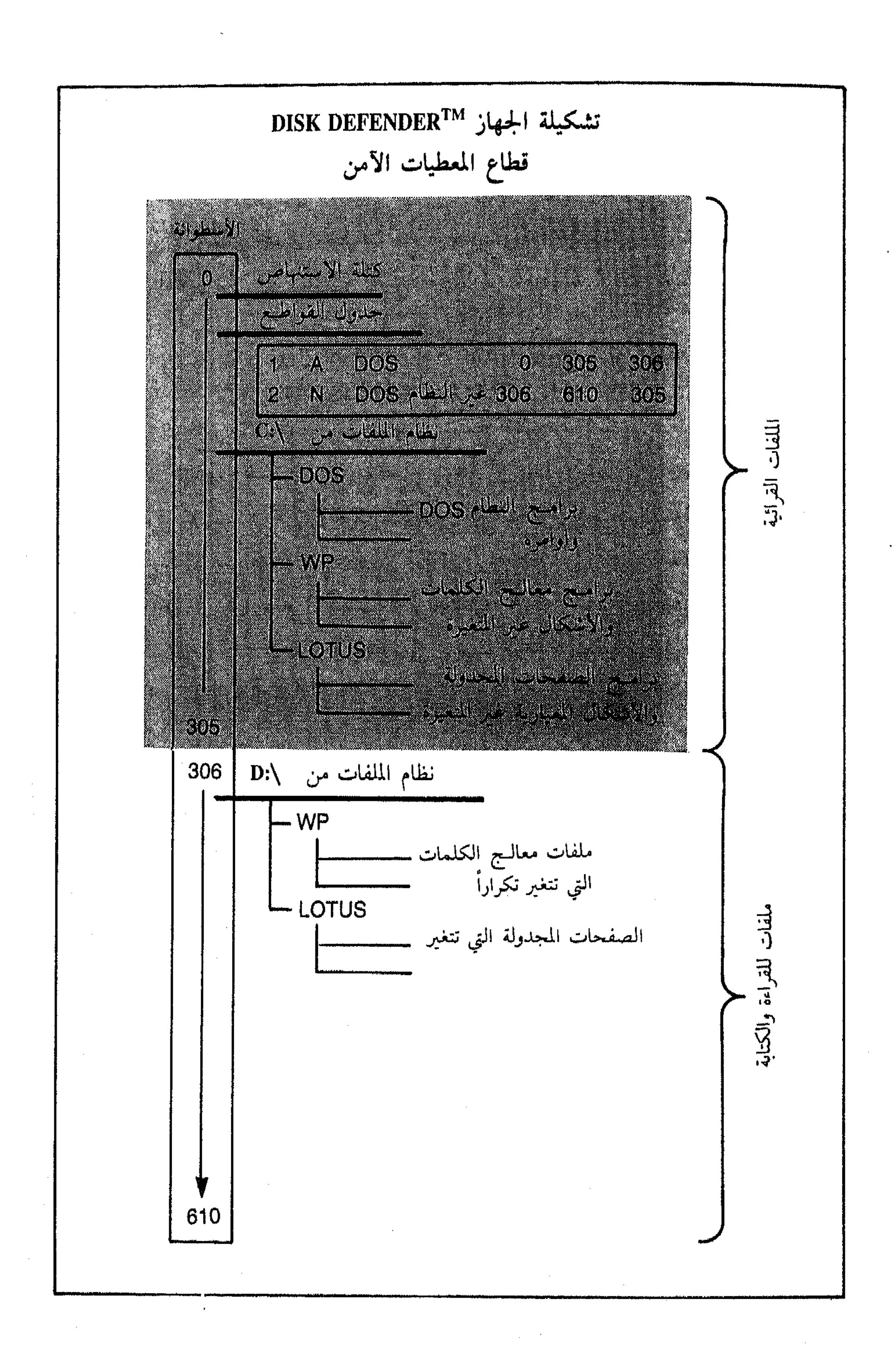
تطورات تقنية جديدة للوقاية من الفيروس

إن الوقاية الأفضل والأكثر فعالية ضد عدوى الفيروس سوف تتم عندما يجري تغيير البنية التصميمية للحواسيب تغييراً جذرياً لتوفير محيط حوسبة لا تستطيع البرامج الذاتية التناسخ من العيش داخله والتكاثر. والنظام OS/2 قد يكون خطوة في ذلك الاتجاه خاصة مع قدراته في معالجة المهمات المتعددة التي تجعل من الممكن تشغيل برامج مضادة للفيروسات في الجهة الخلفية جاهزة للإنقضاض والمدافعة عن معطياتك في حال التعرف على نشاط فيروسي.

الجهاز العتادي Disk Defender الذي اخترعه Dennis Director يدل على خطوة أخرى في الاتجاه الصحيح بالنسبة لحماية أنظمة التشغيل الموجودة للماكنتوش والحاسوب الشخصي. ولقد طور Director دائرة عتادية بسيطة نوعاً ما تعمل كحاجز يمنع الفيروسات من الوصول إلى قسم من القرص الصلب. وهذا المنتوج سابق لأوانه لأن الجهاز Disk Defender ظهر قبل وصول مشكلة الفيروس إلى حجمها الوبائي الحالي وقبل أن يتم تحسين بعض البرامج التطبيقية الشائعة الاستعمال بشكل يكفي لجعلها تعمل بفعالية بأقل قدر ممكن من عمليات الوصول إلى القرص بهدف الكتابة.

وكما يشير الرسم أدناه لتشكيلة الجهاز Disk Defender فإن وضع ملفات نظام التشغيل والبرنامج التطبيقي في قطاع قرائي من القرص الصلب يحميها من الهجوم الفيروسي. وملفات المعطيات المخزونة خلف الحاجز العتادي الذي ينشئه Disk Defender تكون محمية أيضاً. وهذا يعادل وضع عروة حماية ضد الكتابة على حز القرص المرن ولكنه أكثر مرونة لأنه لا يزال بالإمكان الكتابة على الملفات وتغييرها في قسم من القرص الصلب.

وهذا أسلوب مناسب جدير بالاهتمام من قبل مديري ومستعملي الأنظمة. ويمكن إعداد الحاجز العتادي ليتلاءم مع عدة حالات معينة في محيط تشغيل الماكنتوش والنظام DOS.



تشكيلة الجهاز DISK DEFENDER™
قطاع المعطيات الآمن
الأسطوانة
0
كتلة الاستنهاض
جدول القواطع
1 A DOS 0 305 306
2 N DOS غير النظام 306 610 305
نظام الملفات من C:\
DOS
برامج النظام DOS
وأوامره
WP
برامج معالج الكلمات
والأشكال غير المتغيرة
LOTUS
برامج الصفحات المجدولة
والأشكال المعيارية غير المتغيرة
305
306
نظام الملفات من D:\
WP
ملفات معالج الكلمات
التي تتغير تكراراً
LOTUS
الصفحات المجدولة التي تتغير
610
الملفات القرائية
ملفات للقراءة والكتابة

الوقاية الفضلى ــ المساندة

إن استعمال سياسة مساندة فعالة للمعطيات لن يمنع عدوى الفيروس ولكنها تظل أفضل وسيلة للدفاع لأنها تحافظ على المعطيات وتجعل الاسترداد الكامل للمعطيات ممكناً. وبما أن الفيروسات قد تنتشر إلى النسخ المساندة يجب إبقاء النسخ المساندة على أقراص أو أشرطة تسجيل لا تحتوي سوى معطيات مع وجوب وجود مجموعتين أو ثلاث مجموعات من النسخ المساندة لتخفيض خطر فقدان جميع سجلات المعطيات لأنك قمت بمساندة برنامج الفيروس أيضاً.

إذا كنت تملك معطيات يجب حفظها مثل السجلات الأساسية للشركة أو مخطوطة كتاب فيجب أن تدعم التخزين الإلكتروني للمعطيات بنسخ مطبوعة تقليدية لمعطياتك. وقم بطبعها على الورق بشكل يسهل مسحه. لا تستعمل بنوطاً أو نسقاً تزينية بل حضر نسخة مطبوعة تستعمل نوع حرف وترتيب يمكن قراءتها بدقة من قبل أجهزة المسح الضوئية المتوفرة. إحفظ هذه النسخ في مكان آمن كما يذكر الفصل العاشر. وعندئذٍ وفي حال فقدان جميع المعطيات المحوسبة بسبب عدوى فيروسية أو لسبب آخر يمكنك جلب النسخ المطبوعة وجعل أحدهم يمسحها لك أو شراء ماسح في هذه المرحلة من عملك لإعادة المعطيات إلى شكلها الإلكتروني (في الحاسوب).

ولا يحتاج معظم الأشخاص للذهاب كل هذا الشوط ولكنك سوف تحتاج إلى تعديل الطرق التقليدية لمساندة المعطيات من أجل وقاية ملفاتك في وجه الواقع الجديد الناتج عن خطر العدوى الفيروسية. وإذا لم تكن تملك روتين مساندة أصلاً ولم تعان من خسارة فادحة للمعطيات نتيجة عدوى الفيروس أو غيرها من مشاكل الحاسوب المتعددة فإنك تعتمد على الحظ ولا يجب أن تهدر ولو لحظة أخرى.

رغم أن الأقراص الصلبة هي أجهزة موثوق بها جداً عادةً فإنها سوف تتعطل في وقت من الأوقات، وظهور الفيروسات يزيد عادةً من خطر عدم تخزين عملك سوى على القرص الصلب حتى ولو لفترات قصيرة. وهذا لا يعني بأن التخزين على الأقراص المرنة أكثر أماناً. ما تحتاجه هو وجود سجل مستنسخ واحد على الأقل أو إثنين كاحتياطي. وكيف تحضر النسخ المساندة يعتمد كثيراً على ظروف الحوسبة التي تعمل فيها وعلى ميزانيتك ومدى اعتمادك على المعطيات. ومهما كان الأسلوب المعتمد فلا قيمة له إذا لم يكن عملياً بما يكفي ليستعمل بانتظام، كما لا يولد نسخاً مساندة تمكنك من استرداد معطياتك بسهولة إذا ما خسرتها.

ويملك معظم المستعملين معدات مساندة كافية موجودة أصلاً في نظامهم. وتتابع العمل

المطلوب سهل. قم بحفظ العمل الجاري دورياً على القرص الصلب (أو على القرص المرن إذا لم تكن تملك قرصاً صلباً). ويمكنك إعداد الكثير من البرامج التطبيقية بحيث تحفظ عملك عند فترات منتظمة مرة كل 15 دقيقة على سبيل المثال، أو يمكنك كتابة ملف دفعي لجعل عملية المساندة تتم تلقائياً. ولكن لا تنسى بأن هذه المساندة قد تتعرض للفيروس بنفس السهولة مثل النسخة العاملة الحالية.

قم كل ساعة أو عندما تغير الملفات بوضع نسخة من عملك على قرص آخر (على قرص مرن إذا كانت نسختك الأولى على القرص الصلب أو على قرص مرن آخر إذا لم تكن تملك قرصاً صلباً). أنا أقوم دائماً بتحضير نسختين مساندتين واحدة على القرص المرن حجم $5^1/_4$ إنش في السواقة A والأخرى على القرص المرن حجم $3^1/_2$ إنش في السواقة B. وعندها إذا حصل عطل عتادي أو انقطعت الطاقة أو حصل زلزال أو غيرها من الكوارث وهنالك عمل ملح يستوجب الانتهاء، استطيع استعمال النسخ المساندة على أي حاسوب شخصي أو حاسوب منضدي أو حاسوب نقال. واقوم بمساندة المعطيات المهمة جداً على شكل ملفات نصية ASCII غير منسقة وهذا يسهل عملية استردادها كثيراً كما يمكن نقلها إلى حواسيب الماكنتوش أو إلى نظام تشغيل آخر.

ورغم أن الأقراص الأصلية ــ المحمية ضد الكتابة بالطبع! ــ هي نسخ مساندة نظيفة لبرامجك التطبيقية فمن الأفضل تحضير نسخ مساندة إضافية إذا كنت قد بذلت الكثير من الجهد في تشكيل تلك البرامج التطبيقية لتتلاءم مع احتياجاتك واحتفظ بالنسخ المساندة للبرامج على أقراص غير أقراص مساندة المعطيات. لا تخلط بين البرامج والمعطيات على نفس القرص.

قد تريد بشكل دوري إجراء عملية مساندة أرشيفية للقرص الصلب بأكمله. وهذا العمل متعب وقد يستغرق وقتاً طويلاً حسب كمية المعطيات الموجودة على القرص ولكنك تستطيع تسريع الأمور باستعمال البرامج الخدماتية المختصة بالمساندة المضغوطة. و Fastback Plus و PC Tools والبرنامج Norton Backup في برامج نورتون الخدماتية هي جميعها أمثلة مشهورة على هذا النوع من البرامج الخدماتية للحاسوب الشخصي، كما توجد مجموعة متماثلة لحواسيب الماكنتوش والأنظمة الأخرى.

أكتب وصفاً مناسباً والتاريخ على أقراص المساندة واحفظ نسخة واحدة على الأقل في مكان آمن بعيد عن النظام.

وإذا أردت توفير الوقت ولا تمانع بزيادة مصاريفك فإن إضافة قرص صلب ثاني هو الأسلوب الأنسب لاستنساخ ملفات المعطيات والبرامج. ويمكن وضع هذا العتاد داخل حاسوبك أو وصلة من الخارج بواسطة كبل. والمشكلة الكبيرة هي أن القرص الصلب الثاني

هو عرضة لعدوى الفيروس مثل القرص الأول ولذا قد يكون عديم الفائدة عندما تريد استرداد المعطيات.

قد يكون وسط المساندة الأكثر أمناً هو شريط التسجيل. وأنظمة المساندة على خرطوشات صغيرة سريعة جداً وسهلة الاستعمال واسعارها تواصل الانخفاض مع إزدياد الطلب عليها. وتستطيع أيضاً تحضير نسخ مساندة متعددة على مسجل فيديو عادي نوع Beta أو VHS بواسطة براعجيات خاصة وكبلات توصيل. والسيئة المبيتة لتخزين المعطيات خطياً على أشرطة التسجيل هي عدم التمكن من الوصول العشوائي إليها ولكن هذه السيئة قد تغدو فائدة كبيرة بسبب مساعدتها على الحد من الضرر الذي تلحقه عدوى الفيروس.

ولمنع النسخ المساندة من التسبب بنشر التلويث مجدداً يجب استعمالها بحذر خلال روتين الاستعادة بعد حصول هجوم فيروسي. وتقول الجمعية الصناعية لفيروس الحواسيب (CVIA) بأن تسعة من أصل عشرة أنظمة تتلوث مجدداً في غضون أسبوع. والسبب الرئيسي هو إعادة إدخال الفيروس من قرص مرن ملوث عند محاولة استرجاع المعطيات. ورئيس مجلس إدارة الجمعية جون ماكافي وبعد معاينة الآلاف من الحالات يقول بوجوب الشك بجميع الأقراص المرنة التي وضعت في نظام موبوء خلال السنتين السابقتين.

ولهذا فإن الأقراص التي نستعملها للمساندة يجب نسقها دائماً ووسمها إلكترونياً بالاسم والتاريخ وذلك للتدقيق بها بحثاً عن الفيروسات إذا وجب تشغيلها لاستعادة المعطيات. وجميع التغييرات التي تراها عند الفحص قد تشير إلى أن أقراص المساندة قد تكون ملوثة. والأفضل اعتبار أقراص المساندة ملوثة ونسخ جميع الملفات التنفيذية منها إلى أقراص منسقة حديثاً واستعمالها لاستعادة القرص الصلب.

قد يبدو تنفيذ جميع روتينات الوقاية ضد الفيروسات وحماية المعطيات عملاً مزعجاً ومعقداً ومهدراً للوقت ولكن معظمها هو مجرد إجراءات منطقية لا تسبب بالكثير من الازعاج. ومردود هذه الإجراءات كبير لناحية الوقت والتوفير في التكاليف بالمقارنة مع التعرض لعدوى لفيروس دون التمكن من استعادة المعطيات المهمة، وفي جميع الأحوال فإنها عادات جيدة ينبغي تبنيها. وعندما تغدو عادات متأصلة يصبح بالإمكان القيام بأعمال الحوسبة دون أي شعور بالخوف من خطر التقاط عدوى الفيروس والعواقب المترتبة على ذلك.

8 المجموعة الدولية من أشقياء الحواسيب الفيروسيين

هنالك المئات من فيروسات الحواسيب المختلفة المنتشرة في جميع أنحاء العالم. ويظهر كل يوم نسخاً جديدة من الضغوطات الفيروسية المميزة ومشتقاتها والتي يربو عددها عن الثمانين، والتي حددت في محيط عمل النظام DOS فقط.

ولقد إبتدأ عقد التسعينات بإزدياد حاد في معدل حالات العدوى في حواسيب الماكنتوش. وقد ظهرت فيروسات جديدة واكثر قوة في الماكنتوش لتنضم إلى المجموعة المتنوعة من مشتقات الضغوطات الموجودة في قطاع الحوسبة المتزايد النمو. الضغط الفيروسي nVIR الذي بدأ يلوث حواسيب الماكنتوش في ألمانيا الغربية في العام 1987 تبعه أكثر من 30 نوعاً مختلفاً من فيروسات الماكنتوش التي انتشرت في جميع أنحاء العالم.

> قد يبدأ الفيروس كعمل غير ضار أو نوع من المزاح ولكنه يكتسب قدرات هدامة. ولهذا لا تستطيع تصنيف الفيروس على أنه غير ضار بشكل مطلق.

بعض الفيروسات التي إبتدأت كدعابات بريئة تطورت لتصبح أدوات تدمير شريرة للمعطيات. فالفيروس الذي صنعه أحد التلاميذ الألمان في عيد الميلاد لتسلية أصدقائه انتشر في الشبكة الدولية لشركة IBM ليؤثر على عدة أنظمة منتشرة في عدة بلدان. وهنالك بعض الفيروسات التي تم توقيتها لتعمل عند نهاية هذا الفصل والتي تعطلت صمامات توقيتها وإزدادت قوتها التدميرية. والفيروسات التي كانت موجهة إلى أهداف محددة في أوروبا انتقلت عبر الأقمار الاصطناعية حول العالم لتنشر الفوضى في أنظمة تقع في أوستراليا وكندا واليابان. والضغوطات التي اعتقد في بادىء الأمر بأنها تؤثر على نوع واحد من الملفات ظهرت بعد أيام بخصائص مختلفة عمل صانعوها على تغييرها لجعلها أكثر فعالية في تجنب الإكتشاف.

ولا يمكن تحديد قاعدة عامة بخصوص الفيروسات وذلك لأن هذه الفيروسات الشريرة الدولية تتحرك بسرعة وعلى صعيد عالمي. وهنالك الآن آلاف من الأشخاص من 20 جنسية تقريباً بما فيهم ألمع مهندسي البراجيات في العالم الذين يجرون التجارب على برمجة الفيروسات،

وهم يعملون على تعديل وتغيير شيفرات الفيروسات الموجودة والتدافع على إنشاء أنواع جديدة وجذرية من البرمجة التناسخية وذلك في دوامة من النشاط التقني والفكري. ومن هذه الظاهرة الفريدة فكرياً وتقنياً واجتماعياً قد يخرج طرقاً جديدة جذرية ومفيدة يستطيع فيها الحاسوب خدمتنا. وقد يؤدي من جهة أخرى الإزدياد المضطرد في البرمجة العدائية والهدامة الموجودة مباشرة إلى نقطة الضعف في المجتمع العالمي من مستعملي الحواسيب إلى موجة من الإرهاب العالمي في نطاق معالجة المعلومات.

والمشاكل البراجية تكلف الولايات المتحدة الأميركية بمفردها ما يزيد عن بليون دولار في السنة حسب تقرير لمجلس الشيوخ تحت عنوان «Bugs in the Program» (علل في البرامج). والرقم العالمي قد يكون ضعف ذلك إضافة إلى واقع تزايد معدل المشاكل في البراجيات بسبب الضغوطات الجديدة للفيروسات المصنوعة لتخريب البرامج عمداً. وطالما لا يوجد وسيلة دفاع شاملة وفعالة ضد الفيروسات فإن هذه الاحصائيات سوف تزداد سوءاً مع مواصلة الضغوطات الموجودة تناسخها والتحاق الفيروسات الجديدة بها وزيادة انتشار عدوى الفيروس.

> هنالك مليونا نظام من الحواسيب على الأقل وقعت ضحية العدوى الفيروسية.

ومهما كانت هذه الأرقام العالمية مزعجة فإن الفرد لا يحس بها إلا عندما يتوقف نظام حاسوبه الشخصي ويفقد المعطيات. وتلوث آلاف الأنظمة الغربية ليس له تأثير تلوث نظام واحد يعتمد أسلوب حياتك عليه، أو نظام يعالج معطيات أساسية لصحة أحد أحبائك. وفي العام 1990 كان مليونا نظام قد وقعت ضحية العدوى الفيروسية حسب الجمعية CVIA. ومعظم تلك الأنظمة كانت نوعاً من المآسي بدرجات متفاوتة للأفراد والمؤسسات التي فقدت معطياتها.

إن مجتمعنا الذي يعتمد على الحواسيب هو عرضة لهجوم من قبل أعداء لا نستطيع تعريفهم والذين نلاقي صعوبة كبيرة في فهم نواياهم. والنصيحة التي تقول «اعرف عدوك» لا يمكن إتباعها رغم قدرة تجميع المعلومات الكبيرة التي يمنحنا إياها الحاسوب. وهؤلاء الأعداء كثر وهم يعملون بشكل عشوائي وغير منسق مستعملين نفس التقانة التي يهاجمونها لمنع إكتشافهم.

وما يمكننا جزمه هو ما نعرفه حالياً عن مخربي الحواسيب وهو أن أولئك الذين ينشؤون وينشرون الفيروسات هم بأكثريتهم من الذكور الرجال التي تتراوح أعمارهم من المراهقين إلى أوائل الثلاثين وذوي ذكاء فوق المعدل. ومعظمهم موجود في الدول الغربية الصناعية وأغلبهم من الأشخاص المنعزلين الذين يتفاهمون مع وسائل الاتصال الحاسوبية أكثر من تفاهمهم مع الناس العاديين. وهم يظهرون تصرفات عدائية تجاه المؤسسات التنظيمية المتمثلة بالحكومات والجيوش

والشركات الكبيرة. ومعظم صانعي الفيروسات لا يدفعهم الجشع رغم أن مهاراتهم قد تستغل من قبل أولئك الذين يخططون لاستخدام الطاقة الهدامة للفيروسات للكسب المادي والسياسي.

إضافة إلى هذه العموميات فإن أعداءنا الحاسوبيين يعملون في الخفاء ولا نعرف هويتهم. ولكننا نعرف الأسلحة التي يستعملونها رغم التغير المستمر في العتاد العسكري الدولي للفيروسات الذي يتغير بأنماط مربكة من التطور والإبداع.

وينبع معظم الارباك من الطريقة التي تسمى بها الفيروسات. ولا توجد مؤسسات محترمة كتلك التي تعرف الأجناس النباتية أو الأمراض الطبية بحيث تتعرف على الفيروسات المكتشفة حديثاً وتعطيها اسماً مقبولاً تلقائياً ودولياً. ولهذا السبب يعطي الفيروس الواحد عدة أسماء. ويميل الباحثون في مجال فيروسات الحواسيب إلى الافتراض بأن لقاءهم الأول مع أحد الضغوطات الفيروسية هو إكتشاف فريد من نوعه ولذا يلصقون البرنامج اسماً بالوقت الذي يعطى له اسماً آخر من قبل باحث آخر أو أحد المساهمين في الحوارات التي تتم عبر ألواح الإعلان الحاسوبية عن الهجومات الفيروسية.

ويحصل هذا الأمر كثيراً مع الفيروسات العديدة التي تدخل الولايات المتحدة الأميركية عبر الأقمار الاصطناعية من أوروبا. فهي تبدأ بإسم معين لتكتسب أسماءاً أخرى عند ظهورها على الجانب الآخر من المحيط الأطلسي.

ومصدر ارباك آخر هو أن الفيروس الذي قد يعتقد بأنه جديد لا يكون كذلك في الواقع. وبما أن صانع الفيروس لا يحتاج عند تغيير الفيروس المكتوب سابقاً إلى نفس الوقت المطلوب لكتابة شيفرة فيروسية جديدة فإن مبرمجي الفيروسات يميلون إلى «إعادة تأهيل» الكثير من الفيروسات الموجودة وعدم إضافة شيفرة جديدة إلا عند الحاجة. وقد يبدو الفيروس جديداً بالنسبة لمن يتعرض للنسخة المعدلة للمرة الأولى ولذا يطلق عليه اسماً جديداً.

وفي حالات أخرى يجري دمج عنصرين أو أكثر من الفيروسات لتأليف نوعاً من البرنامج الهجيني الذي يحتفظ بالخصائص الأكثر فعالية لفيروساته «الأم». ويجري توليد النباتات التجارية والمواشي بنفس الطريقة بانتقاء الأصل لإنشاء مولود متطور من الناحية البيولوجية. وقد يتميز مثل هذا الفيروس بآلية عدوى فعالة جداً وبأفضل شيفرات التناسخ وبرمجة تجعله يختبيء بسهولة.

ورغم تواجد عدة تباديل (permutations) والتي لا تختلف كثيراً عن بعضها البعض فإن تسمية هذه النسخ الهجينية تصبح صعبة. ولا يبقى أي ضغط فيروسي نظيفاً وثابتاً طالما أن

حقيقة فيروسية

إن البرامج الامتلاكية آمنة كلياً تقريباً في رزمتها الموضبة المختومة. ورغم أن الفيروسات قد لوّثت أحياناً بعض البراجيات الامتلاكية فإن معظم ناشري البرامج الامتلاكية يتخذون تدابير احترازية صارمة لتخفيف الخطر إلى أدنى حد، وعلى الأقل إلى حد أقل من الخطر الذي تتعرض له البراجيات المشتركة أو براجيات القطاع العام أو البراجيات المقرصنة. ولكن صانعي البراجيات يعرفون بأنهم قد يتعرضون لشتّى أنواع الملاحقات القضائية إذا ما ادعى أحدهم بأنهم ينشرون الفيروسات في براجهم الأصلية الموضبة. ولهذا السبب فإنك لن ترى أبداً رزماً تحمل الوسم «خال من الفيروس» حتى في حالة المنتوجات النظيفة.

جميع أنواع الفيروس المعين قد تمر في أنظمة عدة مهووسي حواسيب لا يستطيعون مقاومة إغراء محاولة تعديلها لجعل قسم من البرمجة أكثر فعالية، أو لتحسين إحدى الروتينات أو إضافة لمستهم الخاصة.

وكما الحال مع البرمجة الجيدة فإن الفيروس يتطور وينضج كلما تم تعديله ولكن لا يوجد معيار يمكن بواسطته اعتبار أحد الفيروسات قد تطور إلى حد أصبح فيه برنامجاً جديداً بالكامل بحيث يستحق اسماً جديداً.

وقد يبدأ الفيروس أيضاً كبرنامج غير ضار أو هدفه المزاح ليتم لاحقاً إضافة قدرات هدامة إليه بحيث يكتسب شخصية مختلفة كلياً رغم احتفاظه باسمه الأصلي. ولهذا لا يمكنك تصنيف الفيروسات على أنها غير ضارة بشكل مطلق واكيد، أو تخمين شخصية الفيروس من الاسم الذي تعرف به. إذا قلت في شهر شباط/فبراير بأن الفيروس Ping Pong غير ضار فقد تقول في آذار/مارس المقبل بأن الكرة المرتدة لهذا البرنامج قد اكتسبت القدرة على إتلاف معطياتك وبذا يصبح ذو شخصية مختلفة كلياً وشريرة.

وزيادة في تعقيد الأمور فإن بعض الفيروسات تظل كما هي ولكنها تملك اسماً مختلفاً بدون أي سبب ظاهر. وإذا كنت تعتقد بأن شجرة العائلة معقدة فلن تستطيع فك رموز العمليات التي تسمى بها الفيروسات.

ولحسن الحظ وبغض النظر عما إذا كانت تملك أسماءاً دقيقة أم لا فمن الممكن تصنيف معظم الفيروسات. وكما شرحنا سابقاً فإن جميع الفيروسات تقريباً تقع ضمن ثلاثة فئات أو مجموعات تحدد بواسطة الخصائص الرئيسية التي تظهرها عند تلوث الأنظمة:

- ملوثات قطاع الاستنهاض التي تنتقل على الأقراص المرنة وتتحكم بأنظمة التشغيل بالتصاقها بقطاعات الاستنهاض في الأقراص.

- ملوثات الأنظمة التي تدخل في ملفات أنظمة التشغيل حيث تتناسخ وتتحكم بطريقة عمل النظام.
- ملوثات التطبيقات الإسمية التي تختبىء في شتى أنواع البرامج التطبيقية وتتحفز عندما يشتغل البرنامج منتهزة الفرص الجديدة للتناسخ واتلاف المعطيات وتغيير طريقة عمل البرامج التي تلوثها.

وتستطيع بعض الفيروسات استعمال الطرق الثلاثة لتلويث الأنظمة.

إضافة إلى تلك الفئات العامة فإن بعض الفيروسات اشتهرت بخبثها المميز والخاص بسبب أعمالها أو بالطريقة التي برمجت بها. ويلي هذا القسم وصفاً لمجموعة من هذه الفيروسات. ويرجى التذكر بأن الفيروسات الموصوفة قد يكون أصبح لها خصائص واسماء مختلفة الآن.

ولا يوجد حتى قبول عام لتعريف عبارة «فيروس الحاسوب». وهنالك باحث أوروبي رائد في هذا المجال يحاول نشر الفكرة التي تقول بأن الفيروس يتوالد مرة واحدة وهذا سبب اختلافه عن البرنامج الدودي (worm program). ولقد اعتمد التعريف المقبول عموماً والمنطقي الذي يقول بأن الفيروس هو مجرد برنامج يتناسخ ذاتياً وذلك كهدف رئيسي مبيت في برمجته. وهذا التعريف يفرق ما بين الفيروسات والبرامج الدودية التي هي عبارة عن روتينات هدامة تصنع لتنتشر في الأنظمة بحثاً عن أهداف معينة. ولكنه لا يملك القدرة على التناسخ الذاتي. وإذا قامت بالتناسخ أو بنسخ نفسها خلال عملها إما صدفة أو عن قصد فإنها تصبح عملياً نوعاً من الفيروس.

ونصل الآن إلى مجموعة الأشقياء الفيروسيين الدوليين وهم مجموعة مختلفة العناصر من البرامج الذاتية التناسخ من جميع أنحاء العالم، تختلف خصائصها ولكنها تستطيع اتلاف معطياتك.

فيروسات محيط تشغيل النظام DOS

سوف نبدأ بفيروسات النظام DOS الأكثر عدداً بسبب شعبية النظام DOS في مجتمع الحواسيب عموماً وفي مجتمع المخربين خصوصاً.

«قاتل الأقراص» أو Disk Killer هو فيروس لقطاع الاستنهاض ومن أكثر الفيروسات التي ظهرت في أواخر العام 1989 ضرراً. وعندما يتحفز يعرض الرسالة التالية:

Disk Killer Version 1.0
from Ogre Computers
now killing disk.
Please do not power
down your system.

وقبل عشرة ثواني من عرض الرسالة يكون قاتل الأقراص قد بدأ عملية نسق منخفضة المستوى للقرص الصلب. وفصل الطاقة مباشرة عند ظهور رسالة التحذير على الشاشة لا ينفع لأن كل ما يوجد على القرص يكون قد اتلف قبل أن تتمكن من القيام بأي عمل.

وقاتل الأقراص قد انتشر بسرعة ولوث العديد من البراجيات الامتلاكية وبالأخص تلك العائدة لشركة معينة رائدة في مجال تصنيع البراجيات والتي اضطرت إلى صنع برنامج استعادة باهظ الثمن واتخاذ الخطوات المناسبة لحماية زبائنها. (إن عدم تحديد اسم الطراز أو المنتوج للبرنامج الامتلاكي الذي التقط عدوى الفيروس هو الأسلوب الأفضل كما يبدو، وذلك لأن الحالات التي تعرفها هي تلك التي كشفت عنها الشركات المصنعة بهدف تقليل الخطر الناتج). والعبرة الواجب أخذها من قاتل الأقراص وغيره من ملوثات البراجيات الامتلاكية هي أن المستعملين لا يجب أن يفترضوا بأن البرنامج التطبيقي الجديد «نظيف» بل يجب فحص جميع البراجيات الجديدة التي تدخل إلى النظام بحثاً عن آثار عدوى.

«المنتقم الأسود» أو Dark Avenger هو ملوث للملفات COM. و EXE. الذي يبدو أنه سوف يغدو مشكلة متفاقمة لأنه شديد التلويث والضرر. والمنتقم الأسود يبحث عن البرامج الجديدة التي يريد تلويثها كلما قام البرنامج التطبيقي بعمل ما، بما في ذلك تلقيم وتنفيذ وتحويل الشيفرة أو المعطيات ما بين الأنظمة.

إذا قمت على سبيل المثال بتلقيم برنامج ملوث من قرص مرن إلى قرص صلب نظيف فقد يتحفز المنتقم الأسود مباشرة. وقد يؤدي حتى مسح القرص الملوث من قبل برنامج لكشف الفيروسات إلى تحفيز الفيروس والتسبب بتلويث النظام.

«الحشرة الصفرية» أو Zerobug هي ملوث آخر للملفات COM. من أوروبا. وهو يقوم بإنشاء واتلاف المعطيات بسرعة وفعالية. ويجب أن نهتم بشكل خاص بهذا الفيروس لأنه يتضمن أساليب جديدة للتغلب على العديد من برامج اكتشاف الفيروس الموجودة حالياً في الأسواق.

تعتمد بعض برامج اكتشاف الفيروسات على مراقبة حجم البرنامج لتحديد حالات العدوى المختبئة. ويقوم العديد من الفيروسات بلصق نفسها والاختباء داخل شيفرة البرامج

التطبيقية مما يؤدي حتماً إلى زيادة حجم هذه البرامج الذي تحدده الشركة المصنعة. ويختبىء فيروس الحشرة الصفرية في البرامج التطبيقية ولكنه لا يكتشف بسبب قيامه بإعادة التفاصيل التعريفية كما كانت سابقاً. وهذه إحدى أكثر الطرق ذكاءاً وفعالية في حجب الفيروس التي ظهرت حتى الآن وذلك لأنها تجعل العديد من البرامج والوسائل الخدماتية المضادة للفيروسات عقيمة وبالأخص تلك التي تعتمد على مجموع التدقيق واللقطات أو غيرها من الأدوات التي تقارن الحالة الراهنة للبرنامج مع المواصفات الأصلية بحثاً عن عوارض عدوى الفيروس.

«الاباما» أو Alabama هو فيروس يلوث الملفات COM. و EXE. والتي ادخلت أداة جديدة مزعجة. فكلما تم نسخ الملفات أو تحفيزها بطريقة أو بأخرى في نظام ملوث يقوم الفيروس «الاباما» بتغيير أسمائها إلى اسم ملف آخر موجود على النظام الضحية. ويؤدي ذلك إلى حصول فوضى في سرد ملفات المعطيات بحيث تظل المعطيات موجودة ولكنك لا تستطيع الوصول إليها بفعالية لأنك لا تعرف اسم الملف حيث توجد تلك المعطيات.

وهذا العمل قد يؤدي إلى إرباك وإرهاق أعصاب المستعمل كثيراً بالأخص أولئك الذين لا يزالون يلاقون صعوبة في العمل مع الحواسيب. وعامل إرهاق أعصاب المستعمل قد يكون كبيراً عندما يحصل هذا العمل الهجومي وغير المتوقع والذي يبدو بلا حل عندما تكون متعباً، أو عندما يتلف قدر كبير من المعطيات. وهذا مماثل لقيام أحدهم باستغفالك والكبس على مفتاح الحذف وهدر عملك. قد تكون ردة فعلك مزيج من الألم والعدائية والرغبة بالرد لو كان العمل صادر عن شخص يقف أمامك. ونفس هذه المشاعر سوف تصدر عنك عندما تقوم الآلة التي تعتمد عليها لتعمل بشكل منطقي وموثوق وحسب تعليماتك، بالتهام معطياتك فجأة.

وعوامل إرهاق الأعصاب وغيرها من المشاعر السلبية سوف تكون أكثر حدة عندما يكون المهاجم مخفي وغير معروف. وعواقب الهجوم الفيروسي أو الخوف منها على العلاقة ما بين الإنسان والحواسيب مهمة جداً ولكن هنالك القليل جداً من المعلومات حول هذا الموضوع المهم. والفيروس «الاباما» والفيروسات المشابهة التي تسبب بمشاعر الغضب والإرباك في ضحاياها تضيف بعداً آخراً إلى موضوع الفيروسات يمثل تحدي إداري مهم.

الفيروس **«يانكي دودل»** أو Yankee Doodle هو فيروس غير ضار لحسن الحظ بشكله الأصلي. وهو يحفز عندما تصل الساعة الداخلية للحاسوب إلى الساعة الخامسة بعد الظهر ويؤدي إلى عزف اللحن «Yankee Doodle Dandy» عبر مكبر صوت الحاسوب. ولم يؤدّ هذا الفيروس حتى الآن إلى اتلاف المعطيات أو إلى زيادة حمل الأنظمة عبر التناسخ الجنوني.

الفيروس **«لا شيء»** أو «Do Nothing» بدأ كفيروس غير ضار يلوث الملفات COM. و EXE. دون اتلاف المعطيات أو تحميل الأنظمة عبر التناسخ المتكرر عاملاً مثل المسدس غير

المحشو. وحقيقة عدم قيامه بأي عمل سوى اقحام نفسه بفعالية إلى داخل الملفات COM. و EXE. يجعله أداة مناسبة لحمل فيروس شرير معه.

فيروس «القدس» أو Jerusalem (ويسمى أيضاً بفيروس «الجمعة يوم 13») هو فيروس متناسخ فعال انتشر بسرعة منذ اكتشافه لأول مرة في العام 1987 وهو مسؤول حتى الآن عن حوالي 60 بالمئة أو أكثر من حالات تلوث محيط تشغيل الحواسيب الشخصية.

وإذا التقط نظامك عدوى فيروسية فإنه على الأرجح نوعاً من فيروس القدس. ولحسن الحظ وبسبب انتشاره الكبير ووجوده منذ فترة طويلة فإن معظم البراجيات المضادة للفيروسات سوف تلتقط على الأقل الأنواع الشائعة أو القديمة من فيروس القدس. والبرنامج المضاد الذي لا يفعل ذلك ليس ببرنامج جيد.

وفيروس القدس ابتدأ بالانتشار من الجامعة العبرية في القدس وسرعان ما انتشر في أنظمة أخرى.

وهذا الفيروس يلوث الملفات COM. و EXE. والنسخة الأكثر انتشاراً منه لا تزال تحتوي على علة تجعله يعاود تلويث الملفات EXE. التي سبق ولوثها. وهكذا يتم تعريض النظام الملوث إلى حمل زائد ليتوقف كلياً قبل تاريخ تحفيزه المبرمج والذي يصادف نهار الجمعة في اليوم الثالث عشر من الشهر (الذي يحصل مرة واحدة في السنة). أحد التقارير افاد بأن التحميل الزائد ادى في مدينة واحدة إلى ضياع 7000 ساعة عمل.

الفيروس **Jerusalem-C** هو نسخة لهذا الفيروس والتي لا تملك هذه العلة بحيث تتعرف على الملفات EXE. التي سبق ولوثتها. ولهذا السبب فإنه لا يفقد السيطرة بحيث يحذر من وجوده بسبب أعمال التناسخ. وهذا التحسين يجعله أكثر خطراً من الفيروس الأصلي لأنه يملك فترة «حضانة» أطول تمكنه من تلويث المزيد من الأنظمة.

وهنالك فيروس «القدس الجديد» أو **New Jerusalem** أو **Jerusalem-D** لا يملك التأخير الزمني للنسخة الأصلية. وهو يبدأ باتلاف المعطيات مباشرة ولا يعطي تحذير مسبق عن بدء العدوى.

فيروس **الأحد** أو Sunday هو نسخة أخرى من فيروس القدس تستخدم شيفرة التناسخ والتلويث الشديدة الفعالية لفيروس القدس. وكما يشير اسمه فإن فيروس الأحد يتحفز عندما تصل الساعة الداخلية للنظام الملوث إلى يوم الأحد. وعندما يتحفز الفيروس يرحب المستعمل بالرسالة التالية:

Today is Sunday. Why are you working?
All work and no play make you a dull boy.

وقبل عرض الرسالة أو خلالها يكون الفيروس قد اتلف قسم جداول تخصيص الملفات FAT لنظام التشغيل بحيث لا يمكن إيجاد الملفات. وكما الحال مع فيروس القدس الذي يملك آلية تلويث فعالة بحيث أصبح أكثر الفيروسات انتشاراً فإن فيروس الأحد يتوقع له بأن ينتشر بسرعة في الأنظمة الخاصة وأنظمة الشركات في جميع البلدان المتطورة.

المزيد من الأخبار السيئة عن فيروس القدس: قد لا نكون قد تعرضنا لجميع ما في جعبة هذا الفيروس من اذى وذلك لوجود نسخ منه أكثر ضرراً مضبطة لتحفز عند تواريخ مختلفة من التسعينات. وهنالك نظرية يتداولها بعض صانعي الفيروسات تقول بأن الفيروس المثالي سوف يقوم بتلويث أكبر عدد من الأنظمة قبل قيامه بأي عمل مضر. وقنبلته الموقوتة تضبط لتنفجر بعد عدة سنوات بحيث يتسنى له الوقت الكافي للانتشار في الملايين من الأنظمة.

وأحد نسخ فيروس القدس الذي يملك عدة اسماء مختلفة منها الاسم المناسب **Century** (القرن) يتلاءم مع هذه المواصفات فهو مضبط ليتحفز في أول كانون الثاني عام 2000. وقبل ظهور الكلمات:

Welcome to the 21st Century

على الشاشة يقوم الفيروس Century بإتلاف جدول تخصيص الملفات ثم يكتب اصفاراً في جميع قطاعات الأقراص. (تستعمل بعض المؤسسات العسكرية والأبحاث هذا الأسلوب في كتابة الأصفار لإزالة تلويث سواقات الأقراص الصلبة بالكامل لأن ذلك أكثر فعالية من إعادة نسق عند اتلاف المعطيات على أوساط التخزين المغنطيسية).

وبالطبع يمكن تعديل الفيروس Century لتغيير وقت تحفيزه، وقد حصل ذلك فعلاً. ويؤمل بأن يكون قد تم تطوير عتاد وبراجيات فعالة مضادة للفيروسات قبل العام 2000 من أجل إلغاء فعالية الفيروس Century الأصلي إذا كان قد نجح في الانتشار في الملايين من الأنظمة.

ويتواصل ظهور تنويعات جديدة من فيروس القدس وكذلك بعض النسخ القديمة التي تبدو كأنها جديدة وذلك بأسماء جديدة. وهذه تشمل الفيروس Black Hole و Russian. وهنالك نسخة أيضاً تحفزها روتينات المساندة وهي خدعة قذرة فعلاً.

والفيروس **Friday the 13th** غالباً ما يخلط بينه وبين فيروس القدس لناحية الاسم لأن الإثنين يحفزان يوم الجمعة الموافق في 13 من الشهر. وهو يقوم باتلاف البرمجة عند تفعيله ولكنه لا يواصل التناسخ غير المضبوط كما الحال مع فيروس القدس.

وقد ابلغ عن النسخة الأصلية لهذا الفيروس لأول مرة في أفريقيا الجنوبية عام 1987 ولكنها سرعان ما انتشرت في عدة بلدان أخرى بحيث لا يمكن جزم بلد المنشأ. وهذا الفيروس

يضرب ثلاثة ملفات COM. ثم يتوقف عن العمل. والعديد من ضحاياه يتحسسون وجوده عندما يضيء مصباح السواقة A بعد تلويث الفيروس للفين من الملف COM. على القرص الصلب. ولكن يكون الأوان قد فات للقيام بأي عمل.

ويمكنك توقع الاسوأ إذا ما شاهدت الرسالة المؤدية التالية على مرقابك:

We hope we haven't inconvenienced you.

لقد وضعت هذه الرسالة في نسخة من الجيل الثاني للفيروس Friday the 13th بإمكانها تلويث جميع الملفات الموجودة في الدليل الفرعي الذي تستعمله حالياً، وقد يفلت ليعيث الفساد في جميع الملفات إذا ما استطاع الوصول إلى الأدلة الموجودة في مسار النظام والدليل الجذري.

الفيروس **Ping Pong** (كرة الطاولة) المعروف أيضاً باسم **Bouncing Ball** (الكرة المرتدة) أو **Italian** (الفيروس الإيطالي) أو **Vera Cruz** هو فيروس يلوث قطاع الاستنهاض والذي يواصل ظهوره في العديد من أنظمة الشركات. والكرة المرتدة على الشاشة يبدو كأنها العارض الوحيد للتلوث. ولكن هنالك بعض النسخ التي تملك علة في برمجتها تؤدي إلى الكتابة فوق الجدول FAT في حالة من كل ثمان حالات من العدوى مما يسبب بالتوقف الكلي للنظام وفقدان المعطيات.

وإعادة استنهاض النظام يكفي عادة للتخلص من فيروس كرة الطاولة هذا. والنسخ القديمة لهذا الفيروس لم تلوث سوى الأقراص المرنة ولكن النسخ الأحدث لنفس الفيروس باستطاعتها الحاق الضرر أيضاً بالأقراص الصلبة.

الفيروس **Ghost** (الشبح) الذي ظهر لأول مرة في العام 1990 يخلط بينه وبين فيروس كرة الطائرة لأنه يتميز بكرة مرتدة على الشاشة أيضاً. ولكن الفيروس الشبح يلوث قطاعات الاستنهاض والملفات COM. أيضاً الموجودة على الأقراص الصلبة والمرنة. ولذا يجب، بالإضافة إلى استعمال الأمر SYS لإزالة تلويث قطاع الاستنهاض، إزالة الملفات COM. الملوثة أيضاً.

الفيروس **Columbus Day** (يوم كولومبس) المعروف أيضاً باسم **October 13** (13 تشرين الأول) أو **Datacrime** قام في الواقع بتأدية خدمة لمجتمع الحوسبة في تشرين الأول من العام 1989. فقد قام بتوليد الكثير من الدعاية المسبقة إلى حد جعل العديد من الأشخاص يأخذون وباء الفيروس على محمل من الجد لأول مرة. والمدراء والإداريون بعد قراءتهم عن الفيروس في الصحف بادروا إلى البحث عن الأساليب التي تساعد على تطوير أساليب حوسبة أكثر أماناً والتي سوف تؤدي على الأرجح إلى فوائد طويلة الأمد لجهة حماية أنظمتهم.

وقد حصلت حملة دولية لا سابق لها تهدف إلى إيجاد وإزالة الفيروس من الأنظمة المهمة.

واستطاع خبراء في مكافحة الفيروس من إنقاذ المعطيات في أنظمة مهمة جداً للحكومة السويسرية كانت قد تلوثت، كما تم منع تلف المعطيات أو تخفيفها إلى أكبر قدر في الجامعات وأنظمة السكك الحديدية الوطنية، والمصارف وشركات الإلكترونيات وشركات صنع الأسلحة في أماكن مختلفة مثل فرنسا وأوستراليا إضافة إلى الولايات المتحدة. وخسرت الجمعية الوطنية الملكية للمكفوفين في لندن سجلات مهمة بسبب نشاط فيروسي. ولكن الخوف من أن فيروس يوم كولومبس قد انتشر إلى الآلاف من الحواسيب التي يستعملها المكفوفين لم يكن صحيحاً. والواقع أن تلوث أنظمة الجمعية مثل جميع حالات التلوث الأخرى التي حصلت إبان فترة الذعر التي أحدثها فيروس يوم كولومبس أثبت أنه نتيجة فيروسات أخرى وبالأخص فيروس القدس.

وقد مر 13 تشرين الأول سنة 1989 دون حصول كارثة الحوسبة التي كانت تتوقعها بعض الأوساط الإعلامية مما أدى إلى رد فعل سلبي غير جيد. فقد شعر البعض بأن الإنذار كان خاطئاً وجعلهم يقللون من الخطر الحقيقي الذي تمثله فيروسات الحواسيب.

ولكن فيروس القدس تابع زحفه عبر مجتمع الحوسبة مسبباً حالات جديدة من التلوث كما لو كان يعوض إلى حد ما عن فشل فيروس يوم كولومبس في تحقيق تهديداته سنة 1989. وحتى الآن، فإن فيروس يوم كولومبس يواصل تزايده مثبتاً بأنه لم يفقد عزيمته. وهذا الفيروس يتحفز في يوم من الأيام التي تلي 12 تشرين الأول من كل سنة ولذا احذروه. يزداد حجم البرنامج الملوث بواسطة فيروس يوم كولومبس مقدار 1168 بايتاً وينتج عنه تباطوء في عمل التطبيقات وخسارة المعطيات وإعادة نسق القرص الصلب.

وقد ادعت تقارير الأوساط الإعلامية بأن فيروس يوم كولومبس قد تم اختراعه كبدعة إعلامية لزيادة مبيع الكتب المتعلقة بالفيروس ولكن هذا الأمر مستبعد. فلم يكن هنالك من داع لاختراع فيروس جديد للفت نظر القطاع العام. ولكن السرعة التي انتشرت فيها أخبار ذلك الفيروس ما بين مهووسي الحواسيب في أوروبا والولايات المتحدة تشير إلى إمكانية وجود منظمة تعمل على تنفيذ حملة دعائية حول هذا الفيروس. وقد تكون هذه المنظمة هي «النادي الألماني لفوضى الحواسيب» (Chaos Computer Club of Germany) الرديئة السمعة تحاول لفت الأنظار إليها قبيل مناسبة التجمع الدولي لمهووسي الحواسيب في امستردام، هولندا.

الفيروس **Cascade** أو **Falling Tears** قد لوث حتى الآن عدداً لا بأس به من أنظمة الشركات في عدة بلدان ولكن لا تزال نسبة التعرض للعدوى قليلة. وهو عبارة عن ملوث للملفات COM. يقوم بزيادة حجم البرنامج الملوث بقيمة 1704 بايتاً. والعوارض المرئية لعدوى الفيروس Cascade تتألف من محارف تهبط إلى أسفل الشاشة خلال فقدان المعطيات.

والفيروس Cascade موجود منذ فترة طويلة وهو أساس عدد من الفيروسات المرتبطة قد تحمل نفس الأسم أو قد تسمى الفيروس **1701** أو **1704**. ويدعى **1701** بهذا الاسم لأنه فيروس مقيم في الذاكرة يزيد حجم الملفات COM. بقيمة 1701 بايتاً بينما يعمل الفيروس **1704** بطريقة مختلفة ويضيف 1704 بايتاً. ولزيادة فوضى الاسماء يدعى الفيروس **1704**أيضاً باسم **Blackjack**.

وأفراد هذه العائلة المترابطة من الفيروسات يملكون مزايا مثيرة للاهتمام، إحداها أدى إلى إشاعات مغرضة ولا أساس لها من الصحة بأن مصدر الفيروس هو شركة IBM. ويقوم أحد نسخ الفيروس Cascade بالبحث عن رسالة حقوق الطبع لشركة IBM في جميع الحواسيب التي يدخلها، وإذا اخفق في إيجاد هذه الرسالة التي تشير إلى آلة صنع شركة IBM فإنه يبادر إلى عرض رسائل الشتم واللعن مفترضاً بأنه قد وجد حاسوباً شخصياً مقلداً لحواسيب شركة IBM.

وتستخدم هذه الفيروسات أساليب تجفير (encryption) معقدة ومتطورة جداً تساعدها على تجنب الاكتشاف وتجعل عملية تفكيكها صعبة جداً. ويعقد التشفير إجراءات الاكتشاف وذلك بجعل طريقة التحفيز عشوائية بحيث لا توجد نسختين متطابقتين. ومعظمها لا يتحفز سوى في الأشهر الثلاثة الأخيرة من السنة. والبعض الآخر يتحفز في أول كانون الأول معيداً نسق القرص الصلب ومتلفاً جميع ما يوجد على القرص.

الفيروس Cascade ومشتقاته تواصل تناسخها طوال السنة، وعندما تتحفز فإنها تتصرف بطرق مختلفة ومتنوعة في كل مرة بسبب قيام مخربي الحواسيب بتحسين وتعديل الفيروس Cascade. وتقوم بعض النسخ بمهاجمة أنواع معينة من المراقيب الملونة، والبعض الأخر يسبب بحصول رسالة تحذير للنظام DOS بسبب محاولتها الوصول المتكرر إلى قرص محمي ضد الكتابة.

الفيروس **New Zealand** هو الفيروس المهيمن ما بين الفيروسات التي تعرض رسائل ذات طابع سياسي اجتماعي. وقد بدأ بشكل غير ضار نوعاً ما بعرض الرسالة:

Legalize Marijuana. Your computer is now stoned.

التي تطلب بالسماح بتعاطي حشيشة الماريجوانا. وقد ظهر لأول مرة في نيوزيلندا وهو ملوث لقطاع الاستنهاض واكتسب الاسم **Stoned** بعد وصوله إلى الولايات المتحدة بشكل أكثر عدائية حيث أصبح بمقدوره تلويث الأقراص الصلبة إضافة إلى الأقراص المرنة والتسبب بخسارة المعطيات أيضاً.

الفيروس **Alameda** واشكاله المتنوعة أصبح لعنة الجامعات في الولايات المتحدة. فلقد استعمل التلاميذ المخربون هذا الفيروس كوسيلة للمزاح الإلكتروني اوعملوا على شحذه ليصبح حربة يستعملونها في وجه إدارة الجامعة. وخلال تاريخه المتقلب اكتسب الفيروس

Alameda عدداً من الأسماء المختلفة (مما اعاق تصنيف تباديله المختلفة). وهذه الاسماء تشمل **Merritt** و **Yale** و **Peking** و **Seoul** و **Sacramento** و **SF** و **500** و **Golden Gate** و **Mazatlan**.

والفيروس Alameda الأصلي هو غير ضار ويملك أيضاً آلية مبيتة للتدمير الذاتي. ولا يلوث الفيروس سوى قطاع الاستنهاض لعدد محدود من الأقراص المرنة سعة 360 كيلوبايت. كما يحتوي البرنامج تعليمات مكتوبة تمنعه من تلويث الأنظمة 80286. وقد يكون ذلك نتيجة الافتراض بأن هذه الأنظمة هي الوحيدة التي تستعمل للقيام بأعمال جدية في المرحلة التي كتب فيها هذا الفيروس! وهذه الضوابط المبيتة قد ازيلت تدريجياً في النسخ اللاحقة إلى حد أصبح فيه فيروس Alameda الأخير يستطيع نقل نشاطه بدون أي عائق والتحفيز مباشرة وبدون تأخير، والحاق ضرر كبير بالأقراص الصلبة إضافة إلى الأقراص المرنة.

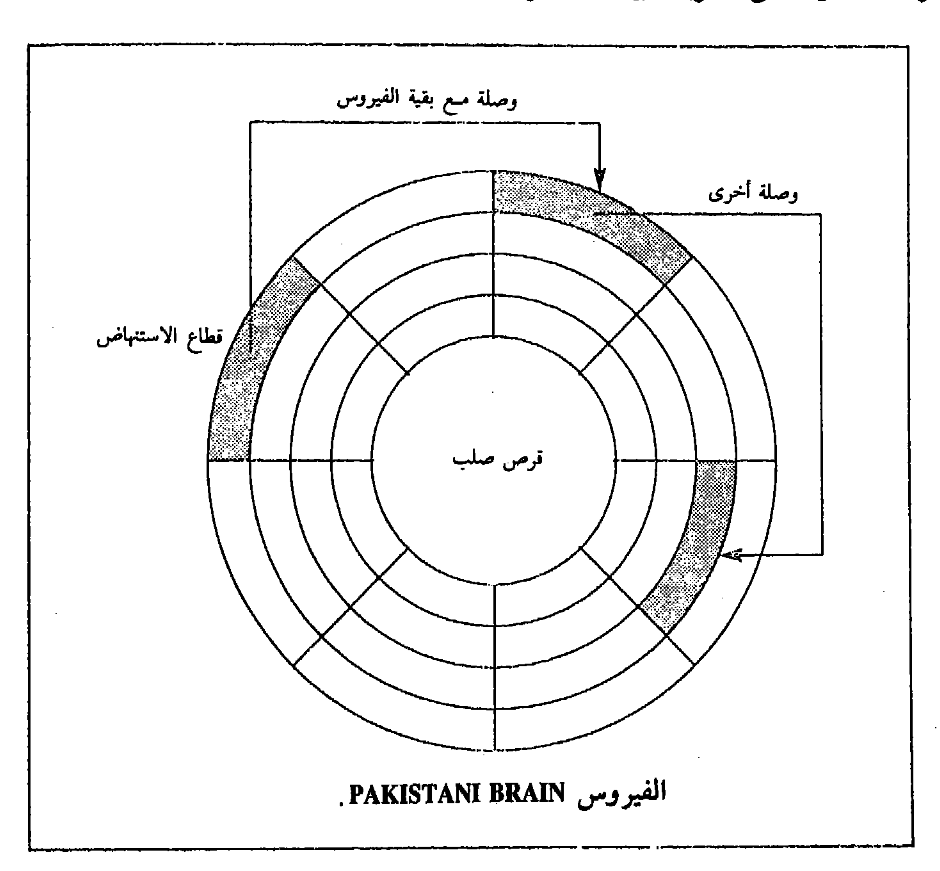
وقبل ظهور فيروس Alameda فإن الفيروس **Lehigh** كان الفيروس الأكثر انتشاراً في الوسط الاكاديمي لأميركا الشمالية. وقد اكتشف لأول مرة في جامعة Lehigh في مدينة Bethlehem في ولاية بنسلفانيا في أواخر العام 1987. ومنذ ذلك الوقت عمل على إتلاف المعطيات من أول البلاد إلى أقصاها مما أظهر مدى السرعة والمساحة التي ينتشر بها الفيروس عن طريق تبادل الأقراص ما بين التلاميذ وأفراد الهيئة التعليمية.

ويقوم الفيروس Lehigh الأصلي بزيادة حجم الملف COMMAND.COM مقدار 20 بايتاً ويغير تاريخ ووقت ساعة وروزنامة النظام ولذا فقد يكتشف المستعمل وجود الفيروس قبل تحفيزه وذلك بعد قيامه بأربع حالات تلويث لاحقة. والعلاج المعتمد لهذا الفيروس الذي خضع لحجم كبير من الدراسات، هو حذف الملف COMMAND.COM الملوث واستبداله بنسخة من قرص نظام التشغيل الأصلي. ولكن لا تتوقع بأن النسخ اللاحقة لهذا الفيروس سوف تتصرف بهذه الطريقة الواضحة والمتوقعة.

هنالك عدد من أوجه التشابه بين الفيروس **Alameda** و الفيروس **Brain** وهو ملوث آخر لقطاع الاستنهاض يسمى أيضاً **Pakistani Brain** أو **Basit** وهما إسمي مخترعيه اللذين طوّراه في مدينة لاهور في الباكستان وهما الوحيدان اللذان وضعا إسمهما وعنوانهما وأرقام هواتفهما في رسالة لحقوق الطبع في الفيروس. ولكن ذلك كان العام 1986 عندما لم تكن الفيروسات قد أصبحت خطراً عاماً قد تعرض المسؤول عنها إلى العقاب. والمعلومات عن مخترعي الفيروس Brain كانت الأكثر حجماً إلى أن اعترف Robert Morris, Jr. من جامعة كورنيل بأنه وراء عدوى شبكات الحواسيب البينية التي انتشرت في المجتمع الأكاديمي ومراكز الأبحاث العلمية في الولايات المتحدة في تشرين الثاني من العام 1988.

لقد قام Basit و Amjad Alvi بتركيب الفيروس Brain على برنامج مقرصن عملا على

بيعه من متجرهما في لاهور والذي يحمل اسم Brain Computer Services . ولم يستطع السائحون مقاومة شراء نسخ من معالج الكلمات WordPerfect وغيره من البراجيات الامتلاكية الشهيرة ببضعة دولارات ولذا تسارعوا إلى شراء الأقراص الملوثة. ويستطيع برنامج واحد من هذه البرامج توليد عدة نسخ أخرى ولذا فإن الفيروس Brain انتشر كالنار في الهشيم في جميع أنحاء العالم وقد أعيدت تسميته باسم **Hard Disk Brain** و **Clone** و **Shoe** و **Houston** كلما ازدادت قدراته على التلويث وإلحاق الضرر.



الفيروس PAKISTANI BRAIN.

وتحتفظ جميع نسخ الفيروس Brain بالأساليب الأصلية الذكية المتمثلة بالتناسخ بسرعة كلما وجدت بيئة مضيافة، وإخفاء نفسها لتجنب الاكتشاف. ويتحكم الفيروس Brain بالنظام عن طريق تلويث قطاع الاستنهاض على القرص ثم يوسع سلطته بشطر نفسه إلى أقسام من البرمجة يتم تخبئتها في مواضع مختلفة من القرص والتي يشار إليها بأنها قطاعات سيئة بحيث لا يستطيع المستعمل قراءتها.

ويعترض الفيروس Brain طريق البرامج الخدماتية التي تمسح قطاع الاستنهاض بحثاً

عن الشوائب ويوجهها إلى قطاع الاستنهاض الأصلي بحيث تحصل على الجواب الذي تتوقعه. وبهذه الطريقة فإن البرنامج الخدماتي لا يواصل بحثه عن الفيروس. وهذا مماثل لقيام مجموعة من اللصوص باختطاف أحد الأشخاص وعندما يأتي الشرطي إلى باب الشقة يتم جعل الضحية تفتح الباب وتطمئن الشرطي بأن كل شيء على ما يرام لتبديد شكوكه وذلك تحت التهديد من خلف الباب.

ولا يملك الاتحاد السوفياتي العديد من الحواسيب الشخصية ولذا فلا يوجد لديه الكثير من الفيروسات ولكن من المحتم التقاطه لمزيد من الفيروسات القادمة من الغرب كما أننا قد نتعرض إلى المزيد من الفيروسات السوفياتية الصنع وذلك مع تنامي مجتمع مهووسي الحواسيب في الاتحاد السوفياتي. والفيروس الأول صنع روسيا هو الفيروس **UNESCO** أو **DOS-62** وهو ملوث للملفات COM. ظهر لأول مرة في مخيم صيفي للحواسيب جرى برعاية منظمة اليونيسكو. وقد سبب بجعل الأنظمة تعاود الاستنهاض عند تشغيل البرامج الملوثة.

وقد رافق ظهور الفيروس **Internet** والمحاكمة اللاحقة للمسؤول عنه Robert J. Morris, Jr حملة دعائية كبيرة. وقد ادى هذا الفيروس إلى تعطيل 6000 حاسوب في جميع أنحاء الولايات المتحدة. وهذا البرنامج هو أصلاً برنامج دودي اخترعه Morris حول أمن الحواسيب. ولكن البرنامج احتوى على علة برمجة جعلته يتناسخ دون رادع والذي يجعله وفق تعريفنا السابق نوعاً من الفيروسات ولكنه لا يزال يعتبر نوعاً من البرامج الدودية.

والبرمجة المتبعة كانت متطورة وتتضمن أساليب تجفير تساعد على إخفائه مما يثبت بأن التجفير التقليدي لا يشكل حاجزاً ضد الفيروسات بل قد تقوم الفيروسات أيضاً باستغلالها لأغراضها الخاصة. والتجفير هو البرمجة لجعل المعطيات غير مفهومة إلا إذا كنت تملك مفتاح فك رموزها. وهذه العملية غير أساسية بالنسبة للفيروس الذي يستطيع اتلاف المعطيات المجفرة مثل غيرها من المعطيات. وهذه الحادثة كانت أكثر حوادث البرمجة الذاتية التناسخ ضخامة وضرراً في ذلك الوقت وفي أي مكان من العالم. ولكن من الناحية القانونية والتاريخية فإن أهم نتائج الفيروس Internet هي إظهارها مدى صعوبة التعامل مع جرائم الحاسوب عبر الأنظمة القانونية الموجودة حالياً. ولقد اختار المحامون المسؤولون عن الدفاع والنائب العام على اختيار هيئة المحلفين من أشخاص ليسوا خبيرين بموضوع الحاسوب وسرعان ما ضاع المحامون والمحلفون وهيئة المحكمة في خضم تعقيدات التعابير والإجراءات الحاسوبية.

وخلال محاكمة Morris استلم الآلاف من العاملين في مجال الطب والأعمال في أوروبا واستراليا وأفريقيا والولايات المتحدة عبر البريد قرصاً مرناً يحمل العنوان: «AIDS Information Introductory Diskette» وقد ارسل القرص من مكتب في لندن تم هجره لاحقاً. ومن بين

اولئك الذين استلموا القرص اشخاصاً حضروا المؤتمرات الدولية حول مرض «الإيدز» في السويد وكندا إضافة إلى المشتركين في منشورات مشهورة تتناول مواضيع الحواسيب والأعمال.

والمستندات المرفقة مع القرص طلبت إرسال قيمة مالية كترخيص لاستعمالها وذلك إلى عنوان في باناما مما جعل السكوتلنديارد في بريطانيا تبدأ حملة تحقيق ضد الابتزاز. والعنوان مثل جميع خصائص هذا المثال الكلاسيكي لبرامج «حصان طروادة» أثبت أنه خدعة. وهو عمل باهظ الكلفة بلغت مصاريفه مئة ألف دولار أميركي وهو بالتالي سابقة خطيرة في تاريخ نشر البرمجة الهدامة.

والمضحك في الأمر أن البرنامج AIDS لم يكن فيروس للحاسوب كما توقع في البدء بل نوع من حصان طروادة أي مدمر للمعطيات مموه على شكل برنامج. والذين لقموا القرص تم اتلاف الجداول FAT في أقراصهم مما تطلب برنامج خدماتي آخر لاسترداد معطياتهم. وقد ساهمت الدعاية الكبيرة وعدم تناسخ البرنامج على تخفيض الأضرار. ولقد سمعت عن أحد المكاتب الذي استلم مديره القرص ولكنه رماه بانزعاج ولكنه لم يقوم باتلافه. وقام أحد الموظفين بالتقاطه في سلة المهملات وشغله على أحد أنظمة المكتب مسبباً بإتلاف كمية كبيرة من معلومات الشركة المهمة. وهذا المثال يشير إلى أهمية الإتلاف الفعلي لجميع الأقراص العديمة النفع والمشتبه بكونها تحتوي على برمجة عدائية.

ورغم أن اليابان وتايوان وكوريا تصنع حالياً معظم حواسيب العالم فإنهم لم يتعرضوا سوى مؤخراً إلى مجتمع مخربي الحواسيب الذين يخترعون البراجيات الذكية والفيروسات الشريرة الموجودة بكثرة في الولايات المتحدة وأوروبا الغربية. والفيروس الياباني الأول لم يضرب اليابان سوى في أواخر العام 1989 رغم وجود عدة حالات عدوى انتقلت إلى اليابان عبر وصلات الاتصال بالأقمار الاصطناعية التي تربطها بأوروبا والولايات المتحدة.

محيط تشغيل حواسيب الماكنتوش

حتى أواخر العام 1989 لم يكن قد كتب الكثير من الفيروسات لحواسيب الماكنتوش أو الابل وقد ساعد ذلك على حماية اليابان من عدوى الفيروسات الغربية بسبب انتشار هذا النوع من الحواسيب هناك. وهنالك سببان للعدد المنخفض من فيروسات الماكنتوش. السبب الأول هو أن معظم مخربي الحواسيب لا يستعملون الماكنتوش ولذا لا يركزون على اختراع الفيروسات لها. وهذا الأمر ينطبق أيضاً على الحواسيب نوع Amiga وغيرها من أنظمة الحواسيب الشخصية الأخرى الأقل انتشاراً من النظام DOS في مجتمع مخربي الحواسيب. والسبب الثاني هو وجود عدد أقل من حواسيب الماكنتوش في الأسواق مما يخفض من احتمالات انتشار العدوى ما بينها.

ولكن وضع مستعملي الماكنتوش تدهور بسرعة في اوائل العام 1990 مع الازدياد الحاد في حالات التلوث وبالأخص في أنظمة شبكات حواسيب الشركات. وحتى ذلك الحين فإن الفيروسات المهيمنة خارج محيط تشغيل النظام DOS كانت MacMag و Scores و nVIR لحواسيب الماكنتوش والفيروس Amiga لأنظمة الحواسيب Amiga القديمة. والفيروس nVIR وهو ملوث للتطبيقات الأسمية موجود منذ فترة طويلة. وقد ظهر لأول مرة في المانيا سنة 1987 وقد تطور منذ ذلك الوقت إلى 30 نوعاً مختلفاً تعمل على تلويث حواسيب الماكنتوش في جميع أنحاء العالم.

وأحد الأسباب وراء انتشار الفيروسات nVIR بهذا الحجم وتنوعها بهذه الكثرة هو أن الشيفرة المصدرية (تعليمات البرمجة الأصلية) متوفرة للمخربين. وهذا الفيروس كان الأول في تلويث برنامج تجاري عام. وعندما قام بتلويث برنامج تخطيطي تستعمله عدة شركات أصبح لديه ثغرة يستطيع الدخول منها إلى محيط حوسبة الأعمال.

وتختلف عوارض الفيروس nVIR حسب النوع المعين. ومعظمها يسبب بالتوقف الكلي للنظام وبإتلاف المعطيات وفي حال تركيب البرنامج Mac Talk فإنه يعطي رسالة صوتية تقول «Don't panic».

الفيروس **Scores** هو ملوث آخر للتطبيقات الأسمية واسع الانتشار، فالحواسيب في وكالة الفضاء الأميركية ناسا ومجلس الشيوخ الأميركي وعدد من الوكالات الحكومية هي من ضمن الأنظمة التي تعرضت للتلوث. وعوارضه المميزة التي ظهرت لاحقاً في فيروسات الماكنتوش الأخرى تتمثل بتغيير رسم الأيقونات. ويعطي الفيروس Scores أيقونات الماكنتوش التي تمثل الدفاتر والمفكرات شكل أذن كلب.

والفيروس Scores هو المثال الأول على كيفية قيام فيروس معد لضرب هدف معين بهدف الانتقام، بالافلات ونشر الفوضى وتهديد مجتمع حوسبة كامل. ويبدو أنه قد كتب من قبل موظف ساخط وقد سدد بشكل خاص على الأنظمة التي تعالج المعطيات العائدة للشركة العملاقة Electronic Data Systems. وبعد اكتشافه في الشركة EDS في أواخر العام 1987 كان قد بدأ بنشر الفوضى بشكل عشوائي مهاجماً حواسيب الماكنتوش دون تفريق.

والاستعمال المتنامي لحواسيب الماكنتوش في شبكات حواسيب الشركات والنشاطات المتصلة على الخط وتبادل الأقراص التي تحصل خلال أعمال النشر المكتبي تزود فرصاً أكبر لانتشار العدوى. ونظام تشغيل الماكنتوش يفترض بأن لا يكون للمستعمل العادي ولا يحاول استعماله سوى الفضوليين أو المحترفين في استعمال الحواسيب. وهذا الأمر يحد من حجم الفيروسات المصنوعة للماكنتوش ولكنه يضع عائقاً في وجه المستعمل العادي بحيث لا يستطيع

الرد بمهارة فنية على ضربات الفيروس. ولهذا السبب فقد حصل ارتباك في وسط الشركات في اوائل العام 1990 عندما بدأت حواسيب الماكنتوش الأعمالية تسقط الواحدة تلو الأخرى ضحايا للفيروسات **WDEF A** و **WDEF B** التي عدت المحيط الأطلسي من بلجيكا.

والفيروس WDEF يؤثر مباشرة على البرنامج Finder وذلك باتلاف ملفات البرنامج Desktop الخفية والتسبب بحالات توقف كلي متلاحقة عند محاولة التلقيم من القرص. ولا تتأثر الملفات النظامية الأخرى والبرامج التطبيقية وملفات المعطيات كما يبدو. والضغط المتواصل على المفاتيح Option و Command خلال إعادة الاستنهاض يبدو وكأنه يزيل الفيروس في النسخ الأولى من الفيروس WDEF.

إن عالم الماكنتوش معرض جداً لأنواع أخرى من الفيروسات خاصة تلك الموجهة إلى المرفق INIT الذي ينفذ وظائف بدء الشتغيل الأولي التلقائية المماثلة للملفات AUTOEXEC.BAT في عالم النظام DOS. والحافظات (Folders) التي تعادل أدلة ملفات النظام DOS هي منطقة أخرى معرضة للتلوث.

اتجاه تطور فيروس الحواسيب

لقد حصل ازدياد ملحوظ في عدد الفيروسات الدولية المكتوبة. وقد أصبحت أكثر تطوراً من ناحية برمجتها وبالتالي أكثر فعالية في الانتشار لإيجاد أوساط استضافة جديدة من أجل نشر العدوى حالما تصبح داخل النظام المضياف، وكذلك من ناحية التناسخ.

المنتقم **الأسود** هوتطور مهم بحد ذاته لناحية قدرته على مهاجمة البرامج المصممة لاكتشاف الفيروسات بينما **Zerobug** هو الحدث الأول لنوع جديد من شيفرة الاختباء التي تتغلب على العديد من برامج اكتشاف ومكافحة الفيروسات.

وأسلوب الفيروس **Alabama** في تبديل اسماء الملفات يشير إلى أسلوب برمجة الفيروسات الأكثر تطوراً وخداعاً الذي بدأ بالظهور. والاسوأ هو ظهور ملوث للملفات EXE. يقوم مباشرة بإزالة تلوث ملف ملوث حالما يفتحه المستعمل. وهكذا فإن الملف يبدو طبيعياً ولكن حالما يغلق يعاود الفيروس تلويثه.

والتطبيق الأول لهذا الأسلوب الذي يجعل الفيروس خفياً كان في الفيروس **4096** الذي أدى إلى الحث على إجراء الكثير من الأبحاث على جانبي المحيط الأطلسي. ومن المؤسف القول بأنه مؤشر على مدى التطور والأذى الذي سوف تصبح عليه الفيروسات في المستقبل.

9 تأثير الفيروس على مستقبل الحوسبة

إن الانتشار الواسـع للبرامـج العدائية الذاتية التناسـخ لها تأثير كبير جداً على مستقبل الحوسبة بأكمله. وبعض هذه التأثيرات ظاهر بينها البعض الآخر افتراضي. ولكن الواقـع القاسي يشير إلى أن الفيروسات هي بنفس قوة البرامجيات العادية. وتوقعاتنا الإيجابية الحالية لما تستطيـع تقانة الحواسيب القيام به سوف تعاق نتيجة معرفتنا بأن الفيروسات وغيرها من البرامجيات العدائية بإمكانها التسبب بنتائـج سلبية كبيرة لها نفس الأبعاد.

> الحقيقة المرة تشير إلى أن الفيروسات تملك نفس قدرات البرامجيات العادية.

وإحدى هذه التوقعات تشير إلى أن الفيروسات والمخاطر التي تحملها لا يمكن التعامل معها بنفس الأسلوب المعتدل السابق. ويجب أن يواجه مجتمـع الحوسبة بأكمله حقيقة الفيروسات كلما أصبـح التلوث بالفيروس هو المعيار وليس العكس. والتقييم الواقعي لحجم المشكلة التي تفرضها الفيروسات إضافة إلى المعلومات الدائمة التحديث وغير المتحيزة سوف تعطى من قبل الأوساط الإعلامية المختصة بالحواسيب كلما تقابل كتابها ومحرريها وجهاً لوجه مـع الاحساس الذي تشعر به ضحايا الفيروس عند إتلاف معطياتهم.

ويبدو من المستغرب للوهلة الأولى من أن معظم المنشورات المختصة بالحوسبة كانت الوسط الإعلامي الأخير الذي أقر بأهمية معظم المشاكل الخطيرة التي تواجهها. وبينما كانت مجلات الحواسيب الكبرى التي تغطي محيط تشغيل الماكنتوش والنظام DOS لا تزال تقلل من خطر الفيروسات فإن الصحافة الأعمالية ومرافق الاتصال والصحف أخذتها على محمل الجد. واضاف المركز الوطني لحالات القلق النفسي في مدينة نيوجرسي فيروسات الحواسيب إلى لائحته التي تضـم 100بند تمثل الأمور الواجب الاهتمام بها في عقد التسعينات مثل مرض الأيدز والمخدرات ومفعول الجنّة (green house) وتلوث الهواء.

وإضافة إلى الجهل وعدم متابعة الحقائق الذي يتميز به المستعملون فإن العديد من أفراد

صحافة الحواسيب انجرفوا في الحماس الذي تشيعه أجواء هذا النوع من الصحافة. ونشر الأخبار السيئة. وحتى التفكير السلبي يتطلب الابتعاد عن التيار العام وتحدي أراء الزملاء والتكلم بجرأة. ولهذا السبب فإن العديد من صحافيي الحواسيب حاولوا التقليل من أهمية الفيروسات كمشكلة متفاقمة خلال الثمانينات بسبب الوهم الذاتي الطاغي على صناعة الحواسيب نفسها خلال مواجهتها أولى مشاكلها الجدية.

نظرة سريعة على تاريخ الحوسبة

لكي نستطيع تقييم المستقبل يجب أن نراجع بعض تطورات الماضي القريب وبالأخص السبب وراء التجاهل الطويل لمشكلة الفيروس من قبل أولئك الذين كان من المتوقع أن يكونوا أول من يحاول معالجتها.

إن تزايد وباء الفيروس داخل أنظمة الشركات والحكومات في أواخر الثمانينات يتصادف مع مرحلة مهمة من مراحل تطور صناعة الحواسيب نفسها وبالأخص في الولايات المتحدة. والدلالات الاقتصادية والتقنية الطويلة الأمد أشارت إلى أن الصناعة تواجه لأول مرة إمكانية نمو أكثر بطئاً وحتى بعض الركود في بعض القطاعات.

والأهم هو أنه كلما نمت الصناعة ونضجت كلما ضعفت روح الإبداع التي كبرت على أساسها مما يزيد من الخطر في المستقبل. والتوعك الذي أدى إلى الكثير من الضرر في صناعة السيارات في ديترويت خلال السبعينات بدأ يظهر في بعض الأسماء في شركات Silicon Valley في أواخر الثمانينات.

وقد عرّضت الصناعة نفسها إلى خسارة الخصائص الخلاقة التي ساعدتها في مراحلها الأولى على جعل الأمور الصغيرة التي ابتدعتها تنقل الحماس من المستثمر إلى المستهلك. ولقد حل محل رواد الحواسيب الذين كانوا يتمتعون بروح المغامرة، جيل من المدراء والإداريين الذين لم تعد تدفعهم الإثارة التي تخلقها هذه التقانة بل الأرباح المادية فقط.

ولم تعد صناعة الحواسيب في يد أشخاص على نفس المستوى مع هذه التقانة. وقد خفت حدة الحماس في العديد من الشركات الكبيرة لتحل محلها أهداف مادية وشخصية. ويحاول القائمون على هذه الصناعة إيهام الجميع بأن المستقبل جيد ولذا لا يحاول أحدهم التكلم بقوة عن الحاجة إلى مكافحة خطر الفيروس المتنامي والذي يبدو أن القليل منهم يفهمه. وقد ترك أمر مكافحة الفيروس إلى أوساط غير تجارية وبالأخص أكاديميي علم الحواسيب في الجامعات والمستعملين العاديين في المجتمع الاعمالي الذين يعانون من عدوى الفيروس.

والدليل على هذه المرحلة المهمة كثيراً من مراحل تطور الحوسبة متوفر في الإصدارات القديمة لمنشورات الحواسيب في أواخر الثمانينات. وكان من الواجب استعمال هذه المنشورات لتبادل المعلومات حول نقاط الحوسبة السلبية والإيجابية. ولكن التغطية الإعلامية لهذا الظهور المهم والمدهش للبرامج الذاتية التناسخ من قبل هذه المنشورات التجارية المدعومة بشكل رئيسي من قبل المصادر الإعلامية للصناعة لم يكن كافياً. والمعلومات الحقيقية حول الفيروسات كانت موجودة في المنشورات الاخبارية لمهووسي الحواسيب وفي الحوارات الإلكترونية ما بين علماء الحوسبة والمستعملين الآخرين لألواح الإعلان الحاسوبية.

وقد نشأ شرخ في الاتصالات خلال عصر المعلومات. وإذا حاول المؤرخون في المستقبل تحديد السبب وراء التجاهل الطويل لهذا التخريب السائد والمتعمد للآلات من قبل المجتمع المعرض للخطر فإنهم سوف يحصلون على وجهات نظر مختلفة لنفس الأحداث من قبل وسائل الإعلام التي تخدم مجتمع الحوسبة. والمصدر الجدير بالاهتمام هي مجلة البريد الإلكتروني المعتدلة **VIRUS-L** التي تصدرها جامعة Lehigh والتي تتناول مواضيع عن فيروسات الحواسيب، وكذلك نظيرها **Comp. virus** وكذلك الخدمة الخاصة بمعلومات الفيروس للجمعية الوطنية لألواح الإعلان الحاسوبية (National Bulletin Board Society). وقد أدى القلق الكبير الذي سببته الفيروسات ما بين المستعملين بحيث أنه على ألواح الإعلان الحاسوبية الثلاثة هذه حصل حجم كبير من حركة الرسائل بحيث لم يكن بالإمكان أرشفتها بشكل صحيح ولهذا قد نخسر أهم السجلات المتعلقة بحقبة مهمة من تاريخنا التقني.

وقد وصلت استغاثات المستعملين إلى القائمين على صناعة الحواسيب دون إحداث أية رد فعل نتيجة ابتعادهم عن الأسلوب القديم القائم على التبادل الحر للمعلومات ومشاركة الأفكار. وعامل التعاون الذي دفع الحوسبة قدماً في الستينات والسبعينات حلت محله السرية والشك ومجموعة من القوانين العقيمة في أواخر الثمانينات مما أدى إلى هوس بحماية حقوق ملكية الأفكار والذي أدى إلى كبح الإبداع.

«هنالك إحساس متزايد بالخوف من أن بعد النظر والحافز اللذان كانا يدفعان الصناعة قدماً قد اختفيا». هذا ما كتبته مجلة PC/Computing في دراسة شاملة لصناعة الحواسيب.

وقد ترك الأمر لوسائل الإعلام العامة للفت انتباه الرأي العام إلى احتمال إحداث الفيروس لأزمة في عالم الحواسيب. والعديد من المؤسسات الكبيرة التي تعتمد كثيراً على الحواسيب بدأت بحماية معطياتها نتيجة ضغط من مدرائهم التنفيذيين بعد قراءة هؤلاء عن موضوع الفيروسات في مجلات مثل The Wall Street أو Times أو Businessweek، رغم أن هذه البادرة كان يجب أن تصدر قبل ذلك عن المجلات المختصة بالحواسيب. وقد ترك الأمر لوسائل

الإعلام العامة لنشر أسئلة خطرة مثل العنوان الذي نشر على الصفحة الأولى لمجلة Newsweek سنة 1990 الذي طرح السؤال التالي: «Can we trust our software? Computers are reliable, but the programs that run them are fraught with peril» الذي يقول: «هل نستطيع الوثوق ببرامجنا؟ إن الحواسيب موثوق بها ولكن البرامج التي تشغلها محفوفة بالمخاطر».

وقد وصفت مجلة Newsweek البرامج بأنها نقطة ضعف ثورة الحواسيب. وقد لفتت مجموعة من المنشورات الاعمالية والعامة الأخرى الانتباه إلى مشاكل عامة خطيرة تتعلق بالحوسبة والتي تتجاهلها الصحافة المختصة:

- الأخطاء في البراجيات القادرة على التسبب بكوارث هي نظرياً أمور محتمة بسبب العدد الكبير من أسطر البرمجة (فوق المليون سطر) في حاسوب طائرة الجمبو.
- إن النظام الوطني الأميركي للتحكم بحركة الطيران الجوي الجديد والذي يعتمد كثيراً على الحواسيب معرض جداً للمشاكل بحيث لم تستطع إدارة الملاحة الفدرالية FAA الإقرار بأنه سوف يعمل في جميع الظروف.
- البراجيات المعدة لمشروع «حرب النجوم» لن تصبح على الأرجح فعالة مئة بالمئة.
- حالات تعطل خدمات الهاتف في جميع أنحاء البلاد نتيجة خلل في البراجيات هو خطر دائم.

وهذه الأمور المقلقة المتعلقة بهشاشة البراجيات المشروعة المعقدة إلى درجة يصعب فيها اختبارها ثم التغاضي عنها من قبل صناعة الحواسيب المثقلة بالمشاكل أصلاً والتي تحاول المحافظة على قوة اندفاعها مما زاد من مخاطر سيطرة البراجيات غير الموثوق بها على الآلات التي يزداد اعتمادنا عليها يوماً بعد يوم.

وفي خضم هذا السيناريو المزعج ظهر وباء فيروس الحواسيب وهو الحدث الأكثر سوءاً. فالتفكير بأن هذه التقنية العجائبية قد تحتوي على خلل أساسي مخيف إلى حد لم يقبل به البدء. وصناعة الحواسيب لم تكن الوحيدة التي أشاحت وجهها عن الخطر. فالعديد من المحترفين في مجال أنظمة المعلومات الإدارية ومعالجة المعطيات الذين تولوا مناصب عالية في الشركات خلال الثمانينات واصلوا التخفيف من أهمية خطر الفيروس لاعتقادهم بأنه أحد التحديات التي تحاول هدم مراكزهم القوية التي وصلوا إليها عبر خبراتهم التقنية.

والعديد من المحترفين من مستعملي الحواسيب قد اكتسبوا القوة والمال لأنهم خلافاً لمعظمنا لم يهابوا تقانة الحواسيب. ولسوء الحظ بالنسبة لهؤلاء الخبراء فإن وباء الفيروس تصادف مع ظهور الحاسوب الشخصي كمركز الثقل الحقيقي لمعالجة المعطيات بالنسبة للعديد من الشركات

مستبدلاً الحواسيب المتوسطة والأيوانية التي يتحكم بها خبراء الحوسبة. والمضحك في الأمر هو أنه في حال لجم مشكلة الفيروس فإنها قد تلغي الكثير من السيطرة التي اكتسبها الأفراد من مستعملي الحواسيب بفضل الحواسيب الشخصية واعادتها إلى الاخصائيين المحترفين.

هل سوف تجبرنا الفيروسات على التضحية بالحوسبة المرنة؟

وهذا يقودنا إلى تنبؤات مزعجة حول المستقبل. وكلما ازداد الإحساس بخطر الفيروسات في المجتمع الاعمالي على مصالح الشركات كلما ازداد الضغط من أجل الحد من الكثير من حرية الحوسبة. ويتضمن العديد من أساليب الحوسبة الآمنة الموصوفة في هذا الكتاب قيوداً على استعمال الحواسيب الشخصية وبالأخص تلك الأساليب المتعلقة بشبكات الحواسيب أو التفاعل مع ألواح الإعلان الحاسوبية. ويتطلب هذا الأمر وسائل تحكم وأشكالاً من أعمال المراقبة التي تتجاوز قدرات ومسؤوليات الأخصائيين المسؤولين عن الأمن والقدرات البشرية في الشركات. وسوف يستعيد أخصائيو الحوسبة الذين سيفرضون هذه القيود وسيشرفون عليها، الكثير من السلطة التي فقدوها عندما انتقلت معالجة المعطيات من أنظمة الحواسيب المتوسطة والأيوانية المركزية إلى الحواسيب المكتبية. وسيكون هنالك نتائج بعيدة المدى على أنواع العتاد والبراجيات التي سوف تطلبها أنظمة الشركات وعلى الطريقة التي تحضر بها الأنظمة وتشغل في المستقبل. والبدائل السلبية الأخرى لإجراءات الأمان الصارمة سوف تشمل أيضاً انخفاضاً في المرونة وسهولة الاستعمال والوصول.

ورغم أن معدل انتشار ثقافة الحوسبة تواصل ارتفاعها فإن المشاكل التي يعانيها معظمنا لناحية عدم الارتياح عند العمل مع هذه التقانة سوف تزداد أيضاً نظراً لتوفير الفيروسات أسباباً محسوسة تجعلنا نخاف من حالة عدم الاستقرار التي تتميز بها الحوسبة في المستقبل.

وهذا العامل الجديد من عدم الاستقرار هو على الأرجح العنصر الأكثر جدية في مستقبل الحوسبة معيداً إلى الأذهان الخوف الذي ساد في الستينات حول اعتمادنا المفرط على الآلات. وقد تضاءل هذا الخوف خلال العقدين الأخيرين من الزمن لأن الآلات برهنت بأنها قادرة وموثوق بها إلى حد جعلنا بالنهاية نقبل بأنها أفضل من الإنسان في بعض المهمات ولذا يجب توليتها المزيد من المسؤوليات لناحية إتخاذ القرارات وتنفيذ الأعمال.

> كلما ازداد اقتناع المجتمع الإعمالي بأن الفيروسات تشكل خطراً كبيراً على مصالح الشركات فإن الضغط للحد من الكثير من حريات الحوسبة سوف يزداد.

والنتيجة كانت تسليم أرواحنا إلى طائرات معقدة إلى حد لا يستطيع شخص واحد فهمها كلياً أو التحكم بجميع وظائفها الميكانيكية والإلكترونية. والربان ومهندس الطيران إذا كان موجوداً لا يملك سوى سلطة تحكم محدودة على تجميع وتقييم المعلومات المتعلقة بآلة الطيران.

والعديد من الآلات التي تتولى مسؤولية الدفاع عنا وكذلك أنظمة الإعاشة الأكثر دقة الموجودة في غرف عمليات المستشفيات أو أجنحة العناية الفائقة تعتمد أيضاً وإلى حد كبير على الحاسوب. وبرمجة بعض من هذه الأنظمة معقد إلى حد يجعلنا نعتمد على الحواسيب لإنشاء البرامج مما يزيد من مخاطر عدوى الفيروس لأنه كلما إزداد تعقيد البرنامج كلما إزدادت صعوبة تحديد العدوى والتعامل معها.

وقد يكون هذا الوضع مقبولاً إذا استطعنا مواصلة الاعتقاد بالمبدأ الأساسي للحوسبة الذي يقول بأنه إذا ما استثنينا الأخطاء البشرية التي لا غنى عنها وبعض حالات سوء التصرف البشري العرضي فإن آلاتنا سوف تقوم بما يطلب منها. ولكن هذا لم يعد مؤكداً منذ زمن طويل. فهنالك الآن احتمال تمرد أي نظام تقريباً إذا ما كان يعتمد على إيعازات براجية قد تتلف بسبب تلوث فيروسي.

بعض السيناريوهات للحلول المستقبلية

قد يعترض بعض المشكلين على السيناريوهات هذه ويقولون بأنها من نسج كتب الخيال العلمي، ولكن يجب التذكر بأن تقانة الحواسيب نفسها تقوم بتحويل الخيال إلى حقيقة. يذكرنا السيد John Walker أحد مؤسسي الشركة الناجحة .Autodesk, Inc بهذا الأمر في المقال «Through The Looking Glass» حيث قال ما معناه« . . . يتألف تاريخ صناعة الحواسيب من سلسلة من الأحلام التي تحققت الواحدة تلو الأخرى والتي اعتبرت في البداية بأنها مجرد فكرة من أفكار الخيال العلمي».

وأحد أعمال الخيال العلمي التنبؤية والتي تعالج مسألة الفيروسات وغيرها من أعمال البرمجة العدائية هي الرواية Trapdoor التي كتبها Bernard J. O'Keefe رئيس مجلس إدارة الشركة العالية التقانة EG & G. ويروي O'Keefe في هذه الرواية قصة فيروس زرعه إرهابيون ويهدف إلى تعطيل جميع الأسلحة النووية الأميركية. وقد تطلب الأمر استعمال جميع الحواسيب الأيوانية في البلاد لمحاولة تحليل وفك شيفرة الفيروس. «لقد كتبت هذه الأقصوصة للإشارة إلى مدى تعقيد التقانة الحديثة ولإظهار كيف أن خطأً واحداً أو قرار خاطىء واحد أو عمل تخريبي واحد إلى سلسلة من الأعمال التي قد تقضي على الحضارة البشرية برمتها» هذا ما كتبه O'Keefe في مقدمة كتابه.

يجب أن نأخذ على محمل من الجد ما قد يبدو اعتقاداً خيالياً علمياً. وخلال التسعينات فإن انتشار فيروسات الحواسيب المتعمد أو العرضي قد يؤدي إلى التطورات التالية:

الأنواع الشائعة الاستعمال من البراجيات التجارية قد تصبح ضحية لأعمال التخريب الصناعية.

إن حالات البراجيات التجارية التي تحتوي على فيروسات يزداد بمعدل مزعج. وقد أصبح من الممكن منذ وقت طويل قيام أحد المنافسين بوضع فيروس في برنامج منافس له دون إكتشافه. وقد انخفض أيضاً احتمال حتى الشك بهذا العمل بسبب ازدياد عدد مصادر التلوث المحتملة ازدياداً كبيراً.

وقد تكون البراجيات التجارية أيضاً هدفاً للموظفين الساخطين أو للعاملين في سوق القطع العالمي وناشري الدعايات والاشاعات وأولئك المشتركين في الدعاوي القضائية المتعلقة بحقوق الطبع وبراءات الاختراع وغيرهم من الأشخاص العدائيين.

قد تحظر بعد البلدان استيراد براجيات الحواسيب من البلدان الأخرى التي تملك مشكلة فيروسات مستفحلة.

«لدينا قوانين حجر صحي صارمة جداً بخصوص الحيوانات والنباتات وغيرها ولكننا لا نملك حجر صحي على براجيات الحواسيب والتي قد يكون تأثيرها أكثر خطراً من أمراض الحيوانات أو الإنسان» هذا ما اخبرتني إياه Colin Keeble من العيادة الاسترالية للفيروسات (Australian Computer Virus Clinic) «وشعوري هو وجوب تدخل الحكومة في هذا الصدد وإنشاء مكاتب لنصح مستعملي الحواسيب الشخصية كيف يحمون أنظمتهم».

سوف تصبح اخلاقيات العمل مع الحواسيب موضوعاً مهماً وسوف تقترح قواعد عمل ومعايير لترخيص العمل وتطبق جزئياً.

وهذه التطورات لن يكون لها تأثيراً كبيراً على الفيروسات ولكنها سوف تنتج فوائد محسوسة عندما تتناول المواضيع الإخلاقية التي يثيرها الذكاء الاصطناعي والتحكم بالمعلومات المحوسبة. والمقررات الإخلاقية مثل المقرر «المعلومات والمجتمع والإنسان» الذي تعطيه جامعة Polytechnic في مدينة بروكلين، نيويورك سوف يصبح أحد المناهج المقررة في معظم مناهج دائرة علم الحواسيب في نهاية هذا العقد.

سوف تتعرض الأنظمة الحساسة كثيراً في الحكومة والخدمات العامة إلى التلوث بالفيروسات على المستوى الوطني والخاص.

لم تعد المعايير الحالية كافية للحماية ضد حالات التلوث الجديدة ويجب تعديلها بشكل

متواصل. وصانعو الفيروسات يواصلون تطويرهم لتكتيكات واسلحة جديدة مما يستوجب إيجاد استراتيجيات جديدة للمحافظة على أمن الحواسيب. والاعتماد على نظام التشغيل UNIX لتوفير الأمن الكافي قد يثبت عدم جدواه وذلك لأن الفيروسات تستغل عناصر الدرع الواقي للنظام UNIX وبالأخص شيفرة إزالة العلل وابواب المصيدة للدخول إلى برامج البريد الإلكتروني. وإضافة إلى ذلك فإن الوكالات الحكومية تزيد من استعمالها لأنظمة DOS والماكنتوش وهي الأكثر عرضة للفيروسات.

ونتائج الإحصاءات السكانية في الولايات المتحدة سوف تكون موضع شك إذا كان هنالك أسباب إلى الاشتباه بتلوث البرامجيات التي تقوم بجمع ومعالجة الاحصاءات. وسوف تنشأ حملة قوية تدعو إلى الامتناع عن أساليب عد الأصوات إلكترونياً خلال الانتخابات والعودة إلى أسلوب الانتخابات اليدوي القديم.

ولقد اطلقت جريدة The New Yorker العام 1988 تحذيراً حول عدم وثوقية الاقتراع الإلكتروني ولكن الولايات المتحدة تبدو أقل اهتماماً من غيرها من البلدان حول مخاطر ما أسماه زعيم المعارضة الهندي «فيزوانات براتاب سنغ» بـ «إلغاء التقانة للحقوق الدستورية». وقد حذر سنغ من الطرق المتعددة بما فيها الفيروس، التي بإمكانها جعل عملية الاقتراع مغشوشة.

وقال «الاختراع هو مسألة ثقة وليست عملية ميكانيكية» وابدى تخوفه من أن الاقتراع الإلكتروني قد يؤدي إلى «اقتراف جريمة بحق الديمقراطية».

والخوف المتزايد حول الفساد المستقبلي لحواسيب الحكومات سوف يؤدي إلى اتخاذ إجراءات صارمة كتلك التي اتخذها مكتب الاحصاء السكاني في العام 1990 حين طلب من المكتبات اتلاف الأقراص الملوثة بفيروس «القدس». وهذه الحادثة اشارت إلى وجود ميل إيجابي مهم هو ازدياد استعمال الأقراص CD-ROM القرائية لتخزين المعطيات. والكتاب الذي يحمل العنوان Country and City Data Books المخزون على قرص CD-ROM والذي شحن مع مواد الاحصاء السكاني الموجودة على أقراص ملوثة بفيروس القدس بقي صالحاً للاستعمال لأن المعطيات القرائية على الأقراص CD-ROM لا يمكنها نشر العدوى.

سوف يؤدي عدد من حالات التلوث الرئيسية في أنظمة الشركات إلى تعطيل النشاطات الأعمالية في قطاعات الصناعة والخدمات والمصارف.

ومثل هذا النوع من الهجوم محتم من الناحية الاحصائية بسبب كثرة الفيروسات المنتشرة حالياً داخل المجتمع الأعمالي. والنتائج المزعجة لهذه العدوى المستقبلية هو اتلاف معطيات المساندة الحيوية لسبب بقاء الفيروسات في الخفاء لفترات طويلة. وهذه المشكلة سوف تنتج عن

بعض حالات التلوث بالفيروس التي حللت للمرة الأولى في العام 1990 والتي تلوث أحد الملفات لتستخدمه كقاعدة داخل النظام ولكنها تزيل تلوث الملف كلما استدعاه المستعمل بحيث يصبح طبيعياً وبالتالي متغلباً على معظم البراجيات التقليدية المضادة للفيروسات.

ولدينا الكثير من الدلائل التي تشير إلى أن العديد من أنظمة الشركات قد تكون ملوثة دون أن ينتبه أحدهم إلى أن معطيات الشركة الأساسية يجري اتلافها في الخفاء.

«والاعتقاد بأن 'هذا لن يحصل لي' لا ينفع فمن الممكن أن تكون قد تعرضت للتلوث دون أن تدري» هذا ما قاله الدكتور Mel Schwartz الحائز على جائزة نوبل والخبير في أمن المعطيات العام 1988. وقال أيضاً «وكما أن المدراء والإداريين هم الأشخاص الذين قدروا قيمة الحواسيب في البداية كذلك يجب أن يبادر هؤلاء الأشخاص أيضاً إلى الحماية ضد حالات الوصول غير المشروعة إلى معطياتهم».

واعلن الدكتور Schwartz في الصحيفة San Francisco Chronicle بأن «عواقب عدم القيام بأي عمل إطلاقاً تزداد يوماً بعد يوم».

ولسوء الحظ فإن الأمر سوف يتطلب سلسلة من حالات التلوث الخطيرة بالفيروس في الشركات الكبيرة قبل أن يأخذ المجتمع الأعمالي هذا التحذير على محمل الجد وإلى حد قد يصل إلى تحسين الإجراءات الحالية غير الكافية مع الأسف والمتمثلة بكلمات المرور والتي استطاع مخربو أنظمة الهاتف منذ زمن طويل التغلب عليها بجهد قليل.

والأهداف الأعمالية الجذابة بشكل خاص هي أنظمة البنوك التي تتحكم بمعطيات حسابات الزبائن وتحويلات الأموال إلكترونياً، وكذلك أنظمة سوق القطع والصرف العالمي والحواسيب والتي تستعملها شركات المواد الكيميائية والنفط.

رأي القطاع العام عن الحواسيب سوف يتغير.

إذا قامت مجلة Times بتكرار الاستفتاء الذي اجرته منذ عقدين بالتعاون مع الجمعيات الفدرالية الأميركية لمعالجة المعلومات (AFIPS) عن رأي القطاع العام في موضوع الحواسيب فإنها سوف تجد انقلاباً كاملاً حول بعض المواضيع الرئيسية والاعتقاد بأن الحواسيب بإمكانها «عدم طاعة» تعليمات الإنسان المعطاة إليها وأنها قد تشكل خطراً حقيقياً على الحرية الشخصية، قد يحل محل الفكرة القائلة بأن الحاسوب هو آلة «مغفلة» اخترعت للقيام بجميع ما يطلب منها.

وعند بداية هذا العقد من الزمن هنالك اثباتات كثيرة تشير إلى أن الرأي العام يتغير تجاه الحواسيب. تقول الباحثة Susan Sontag في كتابها Aids and its Metaphors بأن فيروسات

الحواسيب تثير مخاوفنا البدائية وتضعف ايماننا في ثورة المعلومات مثلما يفعل مرض الإيدز بخلقه وباءاً لا يستطيع الطب الحديث السيطرة عليه.

«لقد بدأ الناس يتكلمون عن الحواسيب كما لو كانت جسيمات معرضة للأمراض». هذا ما كتبه John Markoff في مجلة نيويورك تايمز. «وهذا التغيير في التفكير يلقي الضوء على بعض المواضيع مثل: ما هو المدى الذي نستطيع فيه الاعتماد على أنظمة معالجة المعلومات؟ وما هو مدى الحرية الذي نريده في مجال تبادل المعلومات؟ والأهم هو أن فيروسات الحواسيب تجبرنا على مواجهة احتمال قيامنا باختراع أنظمة قد لا نستطيع في المستقبل التحكم بها».

سوف تواصل الشركات والوكالات الحكومية عدم الاعتراف بأنها معرضة لخطر الفيروسات وترفض الاقرار بأنها تعرضت لحالات تلوث.

إن إخفاء حالات التلوث بالفيروس بسبب الخوف من الدعاية السيئة لطالما كانت مشكلة أساسية خلال وباء الفيروس، ولا يبدو أنها سوف تخف. وقد اظهرت دراسة على 500 مستعمل للحواسيب في بريطانيا في العام 1989 من بينهم موظفين في مصارف وشركات كبيرة، بأن ما يزيد عن 20 بالمئة منهم قد تعرض لتلوث فيروسي. السيد Paul Duffy مدير شركة Computer Protection Services في بريطانيا وهي المؤسسة التي قامت بالدراسة، قال بأن هذه النتيجة غير دقيقة لأن العديد من الضحايا لم يكونوا على علم بأن أنظمتهم قد خرقتها الفيروسات حتى ولو كانوا مستعدين للاعتراف بذلك. وتقدر الجمعية الصناعية لفيروسات الحواسيب (CVIA) بأن نسبة صغيرة جداً من حالات التلوث في الشركات في الولايات المتحدة يتم الإبلاغ عنها. وقد نحتاج إلى جبر الضحايا على الكشف عن حالات التلوث في أنظمتهم مثلما نملك قوانين تتطلب الإبلاغ عن حالات التلوث الجوي وفساد الأطعمة لتحذير الآخرين الذين قد يتأثرون بذلك لإتخاذ التدابير الاحترازية.

إن حجب المعلومات يشوه مدى جدية الخطر الذي تشكله الفيروسات. وبالنسبة للمصارف التي تميل بشكل خاص إلى الانكار بأن أنظمتها قد تعرضت للتلوث لأن ذلك يؤثر على ثقة الناس بالنظام المصرفي الذي يعتمد حالياً وبشكل كامل على معالجة المعطيات إلكترونياً. وعواقب تعطل البراجيات على المؤسسات المالية قد يكون باهظ الكلفة بشكل هائل مما يجعل إخفاؤه أكثر صعوبة. ويتذكر أصحاب المصارف مبلغ الخمسة ملايين دولار من الفوائد فقط التي اضطر بنك نيويورك دفعها لقاء مبلغ 24 بليون دولار اضطر إلى استلافه لتغطية الحسابات التي تأثرت بعلة في البراجيات. وقد تبلغ الكلفة والوقت المطلوبان للتعافي من تلوث فيروسي خطير أكثر من ذلك بكثير.

وكلما ازداد حجم التلوث في أنظمة الشركات يزداد احتمال تسبب التلوث الفيروسي برفع الدعاوى القانونية. فقد تستعمل على سبيل المثال من قبل محامي الدفاع والنيابة العامة لدعم

قضاياهم في المحكمة. هل تستطيع المستشفيات أو الشركات المصنعة للمعدات القول بأن العلاج الذي أدى إلى وفاة المريض كان سببه فيروس حاسوبي أدى إلى تعطيل المعدات بحيث لم يعد باستطاعتهم التحكم بها. وهل يكونون مسؤولين في نظر القضاء إذا ما تقاعسوا عن حماية أنظمتهم بشكل مناسب ضد خروقات الفيروس؟

سوف تنشأ سوابق قضائية مهمة في العقد القادم من الزمن.

إن القوانين الحالية المتعلقة بالفيروسات سوف تكون غير مناسبة على الأرجح بسبب قيام وباء فيروس الحواسيب المتزايد بسرعة بتوليد مشاكل جديدة. وسوف يحتاج الأمر إلى تشريعات أكثر بعداً وقوة. ولكن مثل هذه التشريعات قد تهدد الحريات المدنية وقدرتنا على استعمال تقانة الحواسيب إلى أقصى حدودها.

سوف يتزايد عدد مخربي الحواسيب وسوف يزداد نشاطهم في إنشاء ونشر البرامج الفيروسية.

ويبدو أن هذا المنحى حتمي. وهنالك جيل كامل من الناس بدأ يظهر تتوفر له الحواسيب بسهولة وبمعلومات أكبر عن كيفية استعمالها. وبنفس الوقت فإن الآراء الأجتماعية القوية عادت لتثير المشاعر ضد المؤسسات السياسية والشركات كما حصل في الستينات. والفيروس هو السلاح الأمثل للاعتراض ضد السلطة والشركات الكبيرة.

وقد تبرهن العاب الثمانينات بأنها ساهمت في التسعينات في زيادة عدد المخربين الذين يستعملون الفيروسات كأسلحة هجومية. وقد حذر البروفسور Gary T. Marx وهو أستاذ في علم الأجتماع في جامعة MIT في مقالة نشرتها مجلة نيويورك تايمز بأن شعبية هذه الألعاب مثل تلك المستعملة للمراقبة الإلكترونية تستطيع «زرع بذور التصرفات اللا اخلاقية وعدم الثقة».

وقد حذر البروفسور Marx أيضاً بأن «هنالك أمثلة تشبه مخربي الحواسيب. فكم من العدد المتزايد من مجرمي الحواسيب الصغار حملوا معهم فكرة استمدوها من لعبة لعبوها في صغرهم لها علاقة بتخريب الحواسيب حيث لا أهمية للأخلاق والمثل وجميع الأمور مجرد تحدي للقدرات الفنية».

ويلفت البروفسور Marx انتباهنا إلى التحذير الذي اطلقه Sinclair Lewis في روايته It Can't Happen Here بأنه إذا تم التعرض للحرية في الولايات المتحدة فإن السبب يكون داخلياً وسوف يحصل بشكل تدريجي.

ومهووسو الحواسيب هم عنصر أساسي في جميع محاولات التنبؤ بالعواقب المستقبلية لفيروسات الحواسيب ويشكلون موضوعاً معقداً. وإذا أردت فهم خطر الفيروس على شركتك أو على حاسوبك الشخصي فإنك تحتاج إلى فهم ذهنية هؤلاء المهووسين أيضاً.

هنالك الكثير من الكلام السخيف الذي يكتب عن مهووسي الحواسيب، وإذا ظل الاعتقاد العام الذي يقول بأن أغلبيتهم هم عامل سلبي سائد فإننا نعرض انفسنا لخسارة قوى الابداع التي تدفع التقانة إلى الأمام. والواقع يشير إلى أنه إذا اردنا ضبط التلوث الفيروسي فإن الحل سوف يأتي على الأرجح من داخل مجتمع مهووسي الحواسيب.

وكما كتبت الدكتورة Sherry Turkle في كتابها المميز The Second Self, Computers and the Human Spirit فإن فهم المهووسين لن يتحقق سوى بدراستهم كأفراد وكجزء من مجموعة تعبر عن احتياجاتها النفسية التي تجسدها في علاقتها مع الحواسيب.

وتقول «بأنهم اسرى هاجس السيطرة التامة على وسط عملهم. وهم مثل عازف البيانو المحترف أو النحات الذي يتعلق بعمله إلى حد الهوس. وهم «مسكونون» بوسط العمل هذا. وهم يسلمون انفسهم له ويعتبرونه الوسط الأكثر تعقيداً ومرونة ومراوغة وتحدياً. ومثلهم الأعلى هو أن الربح الأعظم هو في التغلب على الحوسبة».

وقد كتب هذه الكلمات قبل أن يصبح مهووسو الحواسيب مسحورين بالبرامج الذاتية التناسخ ولكن الفيروسات تجعل ما قالته الدكتورة Turkle صحيحاً. والفيروسات سوف تظل أحد أكثر الأمور الفكرية غرابة في موضوع الحوسبة. وسوف يواصل المزيد من مهووسي الحواسيب تجربتها وإنشاء الفيروسات الجديدة والقوية والتي سوف تفلت إلى عالم الحوسبة عن قصد أو صدفة.

الجانب الجيد هو قيام عدد متزايد من مهووسي الحواسيب باختراع طرق لقهر الفيروسات.

وأحد الأمثلة عن ذلك هو الطريقة التي تدافع فيها المئات من مهووسي الحواسيب في الولايات المتحدة للقيام بمجهود جماعي لقهر البرنامج الدودي Internet. ولقد بدأ مهووسو الحواسيب بتنظيم أنفسهم في مجموعات خاصة من محبذي الإلكترونيات. ولكن هذه الحركة قد تكون لها عواقب سلبية إضافة إلى الحسنات الإيجابية إذا ما استخدم مهووسو الحواسيب «الصالحون» براجيات مضادة للحواسيب فيها بعض العلل والتي قد تصبح أخطر من الفيروسات نفسها. فالبراجيات المضادة للفيروسات كغيرها من البرامج الخدماتية القوية قد تضر كثيراً بالمعطيات إذا ما احتوت على علل أو استعملت استعمالاً خاطئاً.

سوف تستعمل الفيروسات لأعمال الابتزاز.

إن الابتزاز هو أحد المزايا الحالية لجرائم الحواسيب. ولقد كشفت وحدة الأبحاث لصناعة الحواسيب في بريطانيا اثباتات تشير إلى انتشار حالات دفع الفديات لمجرمي الحواسيب كثيراً.

ولقد حذر السكوتلنديارد بأن الإذعان لهذا النوع من الابتزاز قد يعرّض مدراء الشركات إلى توجيه تهم تتعلق بإعاقة سير العدالة.

هنالك تطور جديد سوف يحد من مدى استعداد الشركات في المستقبل للإذعان إلى طلبات الابتزاز والتهديد. ويتمثل هذا التطور باشتراط شركات التأمين بأن تكشف الشركات جميع حالات الاختراق السابقة لأمن حواسيبها قبل أن توافق على إعطائها بوليصة التأمين. وشركة LLoyd للتأمين مثلاً التي تغطي بوليصتها فيروسات الحواسيب تقوم بإلغاء البوليصة إذا لم يتم الإبلاغ عن مثل هذه الخروقات السابقة.

وهذا الأمر سوف يحرج العديد من الشركات في أوروبا والولايات المتحدة التي تعرضت أنظمتها سابقاً لتهديدات المجرمين أومهووسي الحواسيب، أو الـذين لم ينجحوا في اجتياز الامتحان الذي تقوم به «فرق النمور» وهي الفرق التي تنشأها الشركات لتقوم بعملية اختراق لأمن حواسيب الشركة للتأكد من صمودها. وعندما قامت شرطة مدينة لندن بتنفيذ برنامجها Comcheck المتعلق بأمن الحواسيب لاختبار مدى ضعف أنظمة شركات الأعمال اضطرت بعض الشركات إلى شراء برامجيات لحماية أنظمتها وإنشاء الدفاعات قبل أن يتمكنوا حتى من الأشتراك في هذا البرنامـج. أما الآخرين فلم يستطيعوا حتى معرفة عما إذا كان المخربون قد اخترقوا أنظمتهم، وإذا عرفوا ذلك لم يكن لديهم أية وسيلة لمنـع حصول ذلك مجدداً. وقد اخبرني أحد مهووسي الحواسيب البريطانيين عن عطلته المجانية في الولايات المتحدة بدعوة من أحد مؤسسات أبحاث الدفاع. وقال بأن الطريقة الوحيدة ليعرفوا كيف استطعت الدخول إلى نظامهـم كانت بأن يسألوه كيف فعل ذلك. ولكنه أضاف «ولكنني لم أقل لهم كيف سأفعل ذلك في المرة التالية!».

إن مستقبل البرامجيات المشتركة وبرامجيات القطاع العام سوف يهدد نتيجة حالات التلوث الفيروسية الفعلية والخوف الزائد منها أيضاً.

وهذا الاحتمال سيّىء جداً لأن البرامجيات المشتركة وبرامجيات القطاع العام تؤلف القسم الأفضل من البرمجة بالنسبة لعدد كبير من المستعملين وبأقل كلفة ممكنة. وقد بدأ حصول انخفاض حاد في استعمال البرامجيات المشتركة لأنها ربطت بانتشار عدوى الفيروس. وهذا المنحى لن يضبط إلا إذا قام العاملون مع ألواح الإعلان الحاسوبية والوكالات التي توزع البرامجيات المشتركة وبرامجيات القطاع العام على أقراص باتخاذ تدابير احترازية أكثر تشدداً.

ولكن من الجهة الأخرى فإن سرعة إنشاء وانتشار الفيروسات سوف تجعل من البرامجيات المشتركة المضادة للفيروسات أهم وسائل الدفاع والأكثر فعالية. وألواح الإعلان هي الطريقة الأسرع لمواصلة تحديث البرامجيات المضادة للفيروسات وجعلها متوفرة للمستعملين.

مستقبل ألواح الإعلان الحاسوبية سوف يهدد.

سوف يتواصل انتشار الفيروسات عبر ألواح الإعلان الحاسوبية ولذا فإن مستقبل هذا القطاع السريع النمو (هنالك 30000 لوح إعلان حاسوبي في الولايات المتحدة فقط) في خطر. ولكن ألواح الإعلان الحاسوبية الرئيسية ومرافق الخدمات الوطنية للمعلومات مثل CompuServe و Genie سوف تواصل زيادة إجراءاتها لحماية نفسها ضد حالات التلوث الفيروسية في المستقبل والمحافظة على ثقة المستعمل. أما ألواح الإعلان الحاسوبية الصغيرة المحلية أو الخاصة فسوف تجد صعوبة في مواجهة الفيروسات بحيث لن يتمكن بعضها من مواصلة العمل.

سوف يتزايد استعمال الفيروسات لنشر الأفكار الدعائية والمعلومات المغلوطة.

لقد استعملت الفيروسات في السابق لنشر الأفكار الدعائية. فلقد اخترق برنامج عدائي قد يكون فيروساً أو برنامج دودي في شبكة تحليل فيزياء الفضاء لوكالة ناسا ليقوم بنشر حملة دعائية ضد مكوكات الفضاء التي تحمل حمولات نووية. ألعاب الحاسوب للنازية الجديدة (Neo-Nazi) التي بدأت في ألمانيا والولايات المتحدة معاً منتشرة الآن دولياً وبالإمكان جعلها وسيلة دعائية أكثر قوة بربطها ببرمجة فيروسية تقوم بتوسيع نطاق انتشارها. والبرامج الأولى كانت بدائية ولكنها تواصل تطورها وتحسنها فإحداها تعيد رقمياً تركيب صوت جوزف غوبلز وزير الإعلام النازي.

هنالك عدد من ألواح الإعلان الحاسوبية يستخدمها مشجعو النازية الجديدة والتي إذا ما اقترنت بقدرات إنشاء الفيروسات تعطي قدرة تقنية كبيرة لجميع دعاة العنصرية في العالم. وقد كشف تحقيق قامت به مجلة PC/Computing عن التعصب والعنف الحاسوبي وقائع تشير إلى أن الحركات العنصرية واستعمالها للتقنية الإلكترونية يتزايدان بسرعة. وقد انتهى التقرير بمعلومات مخيفة حول مخططات لإدخال جيل من النازيين الجدد الخبيرين في المجالات الفنية في مناصب عسكرية وحكومية رئيسية بحيث يستطيعون في النهاية «تولي السلطة عبر استعمال التقانة وقوة المعلومات».

وهنالك احتمال توفر الحواسيب وبالتالي فيروسات الحواسيب بقدر كبير لدعاة الأفكار السياسية في أوروبا الشرقية والاتحاد السوفياتي. وقد يميل جميع من لهم أراء سياسية أو دينية أو غيرها من وجهات النظر، إلى استعمال قوة الفيروسات لنشر اعتقاد معين وإلى حد قد يصل إلى تعطيل الاتصالات الصوتية والناسوخ (الفاكس) إضافة إلى وسائل إرسال المعطيات التي تستعمل جميعها البرمجة وبالتالي تكون عرضة لهجوم الفيروس.

ولكن لن تستعمل الفيروسات لنشر الإعلانات التجارية. وقد سبق ونشر فيروس يحمل

رسالة تمجد حسنات طراز معين من الحواسيب ولكن الشركة المصنعة لم تكن المسؤولة على الأرجح لأن ربط نفسها بالفيروس لن يساعد على تعزيز صورة الشركة.

وقد تم لاحقاً تعديل ذلك الفيروس إلى نسخة تحتوي على رسالة تحاول تشويه سمعة أحد الباحثين الأساسيين في موضوع مكافحة الفيروس والذي يبين المدى الذي قد تستعمل فيه الفيروسات لنشر معلومات مغلوطة.

الدعاية المتزايدة وازدياد حالات التعرض لعدوى فيروس الحاسوب سوف تخفض من ثقتنا بأنظمة الاتصالات الإلكترونية ومعالجة المعطيات.

لقد اعتبر في الوسط الأكاديمي أن إنعدام الثقة من قبل المثقفين والباحثين الذي يستعملون شبكات الاتصال بهذه الشبكات هو أحد أكبر العواقب السيئة لحادثة فيروس Internet. ولم يعد بالمقدور في المستقبل إعداد شبكات الاتصال الأكاديمية والمستعملة للأبحاث بحيث تتمتع بأقل قدر ممكن من الأمان دون التضحية بالمرونة وسهولة الاستعمال. والاعتماد على الثقة ما بين مجموعة من المستعملين كبديل لإجراءات الأمن الرسمية لم يعد ممكناً بعد استفحال عدوى الفيروس.

وانعدام الثقة هذا مهم جداً لأن شبكات الاتصال الوطنية الحالية لعبت دوراً كبيراً في رعاية الاتصالات ما بين العلماء في الولايات المتحدة. وإذا فقدوا ثقتهم في تلك الشبكات وتوقفوا عن استعمالها بكثافة كالسابق فإن هذا قد يؤدي مباشرة إلى إبطاء عجلة الأبحاث العلمية والطبية والهندسية.

والشركات التي صرفت الكثير من الوقت والمجهود والمال لجعل العاملين فيها يستعملون الحواسيب بثقة يواجهون اليوم مهمة صعبة لحمل موظفيهم على اعتماد أساليب حوسبة أكثر أمناً دون جعلهم يفقدون ثقتهم بنظام الشركة.

ولقد لاحظت مجلة Science News كيف أن فقدان الثقة كان أحد العواقب المهمة لانتشار الفيروسات ما بين مجتمع حوسبة الماكنتوش حيث اعتاد المستعملون العمل في جو من الثقة مع آلاتهم التي صممت أصلاً بشاشات عرض ودية تبعث على الثقة.

وفقدان الثقة هذا قد يؤثر على طريقة ربط الأنظمة وكيفية التشارك داخل المؤسسات في استعمال المعدات الباهظة مثل الطابعات اللايزرية. وسوف نصبح على الأرجح أكثر خوفاً في استعمالنا لمكاتب خدمات الحاسوب مثل مراكز النشر المكتبي المنتشرة كثيراً.

شبكات الحواسيب وهي القطاع الأكثر نمواً في مجال الحوسبة سوف يعاق إلى حد ما بسبب خطر الفيروس.

بما أن شبكات الحواسيب هي وسيلة النقل الأساسية لنشر الفيروسات فقد تبدأ إدارات الشركات الإعمالية بطرح الأسئلة حول جدوى الاندفاع وراء تحقيق المزيد من الترابط. وقد يكون تشبيك الحواسيب أداة أعطيت أكثر من قدرها لناحية زيادة إنتاجية العمل. والسبب هو أن الأنظمة المستقبلية يجب إعدادها مع إيلاء جميع جوانب الأمن اهتماماً أكبر وكذلك الأمر بالنسبة لطريقة إدارة المعطيات، مما قد يعيق بعض الفوائد الأساسية لتشبيك الحواسيب.

وسوف يتم الفصل أكثر وأكثر بين المعطيات والبرامج التطبيقية على الشبكات. ومع إزدياد قوة ومرونة الحواسيب الشخصية والبراجيات التي تشغلها فإن العديد من الشبكات سوف تعمل بفعالية أكبر وتصبح أكثر أماناً إذا ما حددت استعمال البراجيات المشتركة أو حتى منعتها بالكامل وحصرت حركة المرور على الشبكة بالمعطيات فقط.

وأحد مناحي التشبيك التي نتوقعها هو إزدياد محطات العمل غير المزودة بسواقات أقراص وذلك لإزالة أحد أسباب التلوث في الأنظمة.

سوف يزداد عدد النساء العاملات في مجال الحوسبة.

وهذا عامل متقلب في تقييم الأثر الذي سوف يتركه الفيروس على مستقبل الحواسيب. إن أغلبية مهووسي الحواسيب هم من الرجال، ورغم أننا نشاهد المزيد من المساهمة النسائية في مجال الحوسبة فإن الرجال لا يزالون أكثر شغفاً وحباً للمغامرة بالنسبة لاستعمال هذه التقانة.

وإذا أمكن اعتبار هذا المنحى السابق مؤشراً يدل على المستقبل فإن الرجال سوف يواصلون الهيمنة على قطاع برمجة الفيروسات وعلى مجتمع مهووسي الحواسيب عموماً. ولكن هنالك ازدياد في عدد النساء اللواتي يعملن في وظائف تتضمن مهام حوسبة. ورغم أن النساء لا يزالون أقلية ما بين المبرمجين وعلماء الحواسيب فإن هذا الوضع بدأ بالتغير. فقد كانت إمرأة على سبيل المثال على رأس فريق يتضمن الكثير من النساء لتحديث برنامج الصفحات الجدولية Lotus 1-2-3 الذائع الصيت.

ورغم عدم توفر الأدلة فإن التأثير النسائي المتنامي في مجال الحوسبة قد يؤثر بشكل خاص على مشكلة الفيروس. وهذا سوف يكون نتيجة التأثير النسائي الذي يؤدي إلى اعطاء المزيد من الأهمية للمواضيع الإنسانية في الحوسبة. واحد الأمثلة المهمة هي صحة المستعمل مثلاً. والفيروسات كما ذكرنا سابقاً هي مشكلة أشخاص أكثر من كونها مشكلة تقنية ولا نستطيع الاستفادة إلا إذا خرجت الحوسبة من نطاق هيمنة الرجال.

والتأثير المتنامي للنساء في العديد من القطاعات التي كان الرجال مهيمنين عليها فتح الباب للعديد من الأمور المهمة. ويؤمل بأن يساعدنا ذلك التأثير أيضاً على فهم مكافحة ظاهرة

الفيروس. ولقد تعلمنا بسرعة عن الكثير من الأوجه التقنية للفيروس ولكننا لا نعي الكثير عن الدوافـع البشرية وراء هذه الفيروسات.

وتعقيد ظاهرة الفيروس تظهر كل يوم في عمليات تبادل المعلومات على ألواح الإعلان الحاسوبية. ونشرت مجلة Harper's Magazine في عددها الصادر في آذار 1990 نتائـج استفتاء إلكتروني حول الموضوع التالي: «هل تخريب الحواسيب جريمة؟» وبالطبـع فإن الفيروسات كانت أحد المواضيـع الرئيسية. وقام الشاعر الغنائي John Perry Barlow الأميركي بالمساهمة في هذا النقاش وكتب ما يدل على الاختلاف العميق في الرأي حول فيروسات الحواسيب ومدلولها الاجتماعي والسياسي. وقد كتب ما معناه:

«إنني لا أدافـع عن فيروسات الحواسيب ولكن يجب على المرء اعتبار قدراتها المتزايدة والقوية الرادعة. وقبل انتهائها فإن «معركة المخدرات» سوف تتحول إلى المعركة الكبرى الفاصلة ما بين محبي الحرية وأولئك التواقين للحرية والتي توفر الفرصة لمهووسي السلطة الذين يريدون عذراً لتخليص أميركا من شرعة حقوق الإنسان. وإذا حصل ذلك فإنني أريد أن أستعمل كافة الوسائل المتاحة لي لتضليل جواسيس السلطة. والفيروس قد يصبـح الأداة الضرورية لاسترجاع حريتنا. وأقول خافوا من الحكومات التي تخاف الحواسيب».

10 عندما يهجم الفيروس أو تزلزل الأرض باشر تنفيذ خطة للكوارث

بعد زلزال ولاية كاليفورنيا الشمالية في 17 تشرين الأول من العام 1989 تعلم آلاف الأفراد والشركات دروساً عن الحقائق الأساسية للحوسبة. وهذه الدروس قد تساعد كثيراً على تطوير استراتيجية حماية المعطيات ضد حالات التلوث بالفيروس والمخاطر الأخرى على صحة تلك المعلومات.

والزلزال الذي سرى مباشرة عبر منطقة Silicon Valley كان أحد أكبر الكوارث الطبيعية التي أحست بها صناعة الحواسيب ومستعملي الحواسيب. وهنالك بعض الفيروسات التي أحدثت بمفردها ضرراً أكثر فداحة في المعطيات ولكن النتائج لم تكن واضحة أومأساوية كنتائج الزلزال.

والزلازل مناسبة أكثر من الفيروسات لتوضيح مبدأ الفعل وردة الفعل ولذا من المفيد استعراض ما حصل خلال الزلزال وبعده لإقناعك بشمل إجراءات احترازية للتعافي من التلوث الفيروسي في استراتيجيتك المتعلقة بالطوارىء والتي تشمل الصواعق والفيروس والموظفين الحاقدين وانسكاب فنجان القهوة والزلازل.

هنالك خمسة دروس يمكن أخذ العبرة منها بالنسبة لحادثة زلزال كاليفورنيا:

1 ــ المعطيات أهم عادة من العتاد الذي يجري معالجتها فيه. ولكن ليس كل المعطيات مهمة وحيوية ويجب أن تحدد الأهمية النسبية للأنواع المختلفة من المعطيات قبل الانتهاء من إعداد استراتيجية حمايتها.

2 ــ فقدان المعطيات أو القدرة على معالجتها قد يساعد على تدهور الأعمال بسرعة. إن حوسبة عملك هو معيار للتقدم ولكن لقاء دفع ثمن جعلك أكثر عرضة للمشاكل في حالة الطوارىء.

3 ــ الخدمات العامة وغيرها من المرافق الخارجية لا يمكن الاعتماد عليها وبالأخص عندما تكون في أمس الحاجة إليها. فلا تستطيع الاعتماد على الكهرباء أو الهاتف أو غيرها من الخدمات والموردين بحيث تحتاج إلى إيجاد حلول خاصة بك في حالات الطوارىء.

4 ــ العواقب الثانوية للكارثة قد تكون أسوأ من الكارثة نفسها.

5 ــ واعتماد الأساليب الذكية والخلاقة له مردوده. والأفكار المبدعة والذكية وغير المعقدة تقنياً إلى حد ما هي الأكثر فعالية. فالحواسيب النقالة والحواسيب الشخصية المقلدة غير الباهظة وحواسيب الماكنتوش القديمة والواح الإعلان الحاسوبية العامة والهاتف الخلوي في سيارتك وحتى القوارب والمركبات المستخدمة لأهداف التسلية قد تصبح عناصر مرنة وعملية وموفرة في خطة الطوارىء المعتمدة لحالات كوارث الاتصال ومعالجة المعطيات.

وهذه الدروس لا تنطبق فقط على الشركات الكبيرة بل تنطبق على المصالح الحرة المؤلفة من شخص واحد يملك حاسوباً شخصياً غير باهظ الكلفة مثلما تنطبق على الشركات الكبيرة التي تملك حاسوباً ايوانياً.

ولقد راقبت خلال بضعة أسابيع جاري الذي يعمل سمكري يتحول من شخص لا يعرف الفرق بين العتاد والبرامجيات إلى شخص يقوم بتطوير قاعدة معطيات حاسوبية رائعة يحتفظ فيها بمعلومات مصلحته المؤلفة من شخص واحد. وهو يستعمل البرنامج Works من شركة مايكروسوفت لحفظ سجلات زبائنه وجردته وجدول مواعيده، وقد وصله مع البرنامج Quicken الذي يقوم بمهام المحاسبة.

وهو يعرف للمرة الأولى في حياته ما هي مصلحته في الواقع وهو يستعمل قدرته الحاسوبية الجديدة لتوسيع نطاق عمله بسرعة. وهذا المثال هو أحد الأمثلة التقليدية التي تبين كيف أن نظام الحاسوب الشخصي يستطيع أن يكون أداة فعالة جداً في المصالح الصغيرة. والخطر بالطبع يكمن بأن هذه المصالح تصبح تعتمد على سجلات معطياتها مثل المصارف بسبب معالجة جميع معطياتها إلكترونياً.

والاعتراف بهذه الاعتمادية والضعف الناتج عن ذلك هو الخطوة الأولى في إنشاء مخطط جهوزية لحالات الطوارىء. وتحديد المعطيات المهمة وحمايتها بفعالية هي الخطوة الثانية.

ما هي المعطيات المهمة؟

هنالك الكثير من قصص الرعب التي حصلت نتيجة الزلزال والتي يرويها أولئك الذين يعانون من التلوث بالفيروس وهي تعطينا نظرة جديدة بالكامل ليس فقط على أهمية المعطيات بل عن فئات المعطيات التي هي مهمة بالفعل من أجل نجاح جميع أنواع الأعمال.

هل تعرف حقاً ما هي المعطيات المهمة جداً في مجال عملك؟ افترض على سبيل المثال بأن هنالك متفجرة في المكتب ولا تملك سوى 30 ثانية لتأخذ من مكتبك المعلومات التي تحتاجها أكثر

من غيرها في حال انفجر المبنى. ماذا تختار؟ إن القرارات الغريزية والفورية التي تقوم بها تحت تأثير الضغط والمتعلقة بالقرص الواجب التقاطه أو الملف الواجب حمله خلال ركضك نحو الباب قد تختلف كثيراً عن الأولويات التي قد تضعها إذا ما فكرت ملياً بالأمر ودون تأثير الضغط.

وقد اثبتت التجارب بعد زلزال كاليفورنيا العام 1989 هذا الأمر. فالعديد من الأشخاص مروا في مرحلتين من التفكير لاتخاذ القرار حول المعطيات المهمة الواجب إنقاذها. المرحلة الأولى حصلت عندما اخلوا المبنى بحالة ذعر عند حصول الهزة الأولى. والمرحلة الثانية بعد أن تسنى لهم الوقت لتقييم المعطيات المهمة الواجب إنقاذها بعدما سمح لهم بالدخول بسرعة مجدداً إلى بعض المباني المتصدعة لإخراج محتوياتها بعد انتهاء الزلزال. (سوف نعطي في هذا الفصل بعض الأساليب العملية لتحديد قيمة المعطيات.

لقد تم إغلاق الآلاف من المباني بعد الزلزال بعضها كإحتياط حتى يتم معاينتها والبعض الآخر لأنها تصدّعت كثيراً إلى حد أعلن أنها غير صالحة للسكن فوراً. وفي أحد الشوارع انقطعت المئات من المصالح الصغيرة عن سجلاتها وحواسيبها لمدة ساعات وايام وحتى أسابيع. وهذا الأمر بالنسبة لبعض المصالح التي لا تزال في طور البداية كانت خبرة مأساوية لم يتعافوا منها حتى الآن.

وعندما سمح للأشخاص بالعودة إلى مكاتبهم فإن ذلك كان لبضعة دقائق فقط ولم يسمح سوى لشخص أو شخصين فقط بالدخول إلى المباني المتضررة. واولئك الذين وضعوا في ذلك الموقف اضطروا لاتخاذ قرارات تقييمية صعبة حول الأمور الأكثر أهمية في المكاتب والواجب إنقاذها. وبعد اتخاذ تلك القرارات أرسلوا موظفيهم لإخراج تلك البنود من مكاتبهم وبسرعة.

وقرارات استرداد السجلات الضرورية وبسرعة ليست ضرورية في حالة الزلازل فقط، فنفس الأوضاع قد تنشأ في حالات الإخلاء الطارئة بغض النظر عما إذا كان السبب هو حريق أو تدفق المياه أو زوبعة أو هجوم لمسلحين! والمعطيات هي الممتلكات الأكثر تعرضاً للخسارة وهي عادةً لا تغطيها شركات التأمين، كما أن قيمتها الفعلية غير محددة بشكل واضح.

وغالباً ما تفقد المعطيات كنتيجة ثانوية للكارثة وليس خلال الكارثة نفسها. وهذا الأمر ينطبق على الزلازل.

شركة بورلند انترناشيونال كانت إحدى الشركات العديدة التي خسرت ملفات معطياتها بعد الزلازل بسبب تدفق المياه من خطوط المياه أو مرشات اطفاء الحرائق. وقد اضطر العاملون في شركة بورلند الانتقال من المبنى لفترة من الوقت ووضع حواسيبهم في قاعة كرة المضرب

التابعة للشركة لكي تجف. وهذه الشركة التي كانت أكثر تضرراً في صناعة الحواسيب من الزلزال تعافت بسرعة كبيرة لأنها كانت تملك خطة جهوزية ضد الكوارث تشتمل على مساندة المعطيات المهمة وحفظها في موقع آخر. وهذه النسخ المساندة مهمة بعد حالة التلوث بالفيروس الصامتة وغير الدراماتيكية بقدر اهميتها عند تصدع وانهيار المبنى.

المخاطر	العواقب المحتملة									
	خلع وكسر	انقطاع التيار الكهربائي	انكسار خطوط الغاز	انقطاع أسلاك الكهرباء	تلوث المياه	حالات تعفن	تلوث بالدخان	تلوث كيميائي	تلوث	خسارة كاملة
	●	●	●	●	●			●	●	●
حريق	●	●					●	●	●	●
تدفق المياه	●	●		●	●	●		●	●	●
مواد خطرة	●				●		●	●	●	●
زوبعة	●	●	●	●	●	●		●	●	●
هجوم نووي	●	●	●	●	●		●	●	●	●
انقطاع أو ارتفاع فجائي للطاقة	●	●								
تخريب / إرهاب	●	●	●	●			●	●	●	●
عاصفة رعدية قوية	●	●		●	●	●	●	●	●	
إعصار	●	●	●	●	●		●	●	●	●
عاصفة شتوية	●	●		●						
براكين	●	●		●						●

وبعض شركات مدينة سان فرنسيسكو الذين لم يتعظوا من حادثة الزلزال ولم يساندوا معطياتهم الأساسية تعرضوا لحادثة مأساوية أخرى بعد بضعة أسابيع عندما توجب إخلاء المكاتب في وسط المدينة التجاري بسبب سقوط رافعة مما أدى إلى تصدع الأبنية المجاورة لها. والاغلاق الاضطراري المؤقت لبنايتين من المكاتب أدى إلى التوقف الكامل لمئة وخمسين شركة. وقد سمح

لكل منها بإرسال موظف أو موظفين إلى المكاتب لمدة 10 أو 20 دقيقة لجلب ما هو مهم منها ليتمكنوا من مواصلة عملهم في مكان آخر.

وفي أعلى لائحة المستوجبات بالنسبة لمندوبي المبيع والمحترفين على الأخص كانت كتب العناوين وبطاقات أسماء الزبائن والعملاء إلى جانب ملفات المعطيات الرئيسية مثل سجلات الرواتب. ولم يستطع أحد حتى مجرد التفكير بإنقاذ العتاد الباهظ الكلفة سوى أولئك الذين يملكون نسخاً مساندة لمعطياتهم المحوسبة في موقع أمن آخر.

والاحساس بالقيمة الحقيقية لأسماء وعناوين الزبائن والعملاء جعلت العديد من الشركات في كاليفورنيا الشمالية يعيدون النظر بحصر مثل هذه المعلومات وتسجيلها على سجلات ورقية فقط من النوع المعرض للتلف. وهنالك فائدة واضحة في حوسبة تلك المعطيات وخاصة بشكل يسمح بوجودها في كل مكان باستعمال حاسوب نقال وبطريقة تجعل من الممكن أيضاً نسخها ونقلها على الجيل الجديد من وحدات الجيب الالكترونية المستعملة لتنظيم الأعمال. (وبالطبع إذا كانت هذه الوحدات الجيبية قادرة على تشغيل البرنامج وبإمكانها الاتصال مع الحواسيب الشخصية فإنها عرضة هي الأخرى للتلوث بالفيروس. ولكن في معظم الأحيان فهي وسائل تخزين آمنة ومناسبة لأنواع معينة من المعطيات طالما تتخذ التدابير الاحترازية للمحافظة على الخصوصية).

وأولئك الذين كان لهم خيار انتقاء العتاد الواجب انقاذه بعد الزلزال اختاروا الحواسيب النقالة وأجهزتها الملحقة. وبسبب تصميمها فإن المعدات النقالة نجت من نشاط الزلزال وأمكن إعادة تشغيلها لاحقاً بقدر قليل من الجهد في مواقع أخرى. وبشكل مماثل وإذا ضرب الفيروس نظام الحاسوب المكتبي لديك وهنالك عمل مستعجل تريد انجازه فإن المرفق الأفضل للطوارىء هو الحاسوب النقال. تستطيع توقيف الحاسوب المكتبي وتشغيل الحاسوب النقال تاركاً مهمة معالجة مشكلة الفيروس إلى وقت آخر.

كيف تعود على الخط عند حصول أزمة؟

إن التخطيط للتعافي بسرعة هو أمر مهم جداً. وهنالك العديـد من العمليات التي تستوجب معاودة العمل بسرعة كبيرة بعد حصول كارثة. وتتعرض المؤسسات المالية والطبية إلى مشاكل كبيرة إذا توقفت عن العمل لساعة أو ساعتين فقط ولكن في هذه الأيام فإن معظم الأعمال تتضرّر كثيراً إذا ما توقفت عن العمل ليوم واحد.

> ... مجرد المحافظة على سلامة المعطيات لا يكفي بل يجب أن توفر الوسائل لمعالجتها أيضاً.

إن المشكلة الأكبر لأولئك الذين يعتمدون على الكهرباء هو أنه بعد حصول عدة أنواع من الحالات الطارئة ينقطع مصدر إمداد الطاقة المعتاد. وقد انقطعت الطاقة بعد الزلزال عن حوالي مليون شخص وذلك لعدة ساعات وحتى لعدة أيام. والبعض الذي يملك مولدات للطوارىء وجد أنها معطوبة أو لا تناسب احتياجاتهم أو موجودة في مباني لا يمكن استعمالها. وهذا الأمر يشدد على الحقيقة الأساسية التي تقول بأن مجرد المحافظة على سلامة المعطيات لا يكفي بل يجب أن توفر الوسائل لمعالجتها أيضاً.

وصحيفة San Francisco chronicle and Examiner هي مثال على شركة كانت يجب أن تحضر نفسها ولكنها لم تفعل ذلك. وقد اضطرت الاعتماد على مولد نقال صغير موجود على مخرج الطوارىء لتغذية سلسلة حواسيب الماكنتوش لديها بالطاقة للقيام بأعمال التنقيح الالكترونية. وقد عنى ذلك أن المحرّرين والمنقّحين اضطروا إلى توقيف برنامج النشر المدمج المتكامل النظام المتطور واستعمال البرنامج MacWrite القديم وتعلم الأسلوب القديم والأقل تطوراً للتنقيح خلال هذه الحالة الطارئة المرهقة للأعصاب. وحتى عادات الحوسبة البسيطة البديهية المطلوبة في النظام العادي قد تجعل النظام المستعمل في حالة الطوارىء يخفق عن العمل. إذا قام مثلاً أحد الصحافيين في صحيفة Chronicle بنسق تقريره على حواسيب الماكنتوش الصغيرة فيصبح من الصعب تحويل النسخة إلى برنامج تنضيد (typesetting). ولكن الصحيفة استطاعت الصدور مبرهنة ما يمكن إنجازه في حالة الطوارىء باستعمال الأدوات البسيطة ولكن كان بالامكان تلافي هذه الصعوبات وهذا الإرهاق لو تم إعداد خطة طوارىء.

وهذا يرسخ اعتقادي بأن أحد أفضل المشتريات بالنسبة لقدرة الحوسبة العملية النقالة والمستعملة كوسيلة دعم هو حاسوب ماكنتوش صغير يمكن شراؤه بأسعار زهيدة. وهذا ما حصل في الواقع مع صحيفة Chronicle بعد زلزال عام 1989 حيث أصبحت خطتها بالنسبة للطوارىء تشتمل على استعمال حواسيب الماكنتوش والحواسيب النقالة بطريقة أكثر تناسقاً وانتظاماً.

ولا تتعرض جميع المؤسسات الإعلامية لهذه المخاطر الطبيعية ولكنها جميعها معرضة لهجوم الفيروس على أنظمة التنقيح الالكترونية لديهم والتي قد تكون نتائجها أسوأ من الكوارث الطبيعية. هنالك على سبيل المثال فيروس واحد على الأقل هدفه أنظمة معالجة الكلمات والتنقيح الالكتروني والذي يضيف الشتائم إلى أسماء بعض الزعماء السياسيين.

وكلما ازداد عدد الفيروسات الموجهة لنشر الآراء ووجهات النظر السياسية كلما ازداد الخطر على أنظمة التنقيح الالكترونية في المؤسسات الاعلامية. والحل الأسرع عند حصول حالة تلوث مع اقتراب موعد الإصدار هو التحول إلى نظام مساند بسيط مصمم بشكل خاص لحالات الكوارث المادية وخاصة إذا كان الموظفون يستطيعون استعمال مثل هذا النظام.

وهنالك حادثة أخرى ذات مغزى بالنسبة لفيروسات الحواسيب توضح الفائدة الكبيرة التي قد توفرها أبسط المرافق الاحتياطية. خلال سريان الهزة الأرضية قوة (7-1) على مقياس ريشتر عبر منطقة Silicon Valley فإن توقيت الهزة أنشأ ما يعادل الكترونياً انقطاع الضوء خلال إجراء عملية في الدماغ وذلك بالنسبة Ari Goretsky المدير الفني لجمعية National Bulletin Board Society و John McAfee رئيس مجلس إدارة الجمعية الصناعية لفيروس الحواسيب وقد كانا في مرحلة حرجة من مراحل تحليل عينة من فيروس الحواسيب «المنتقم الأسود» (Dark Avenger).

وقد بـدا وكـأن القوى التدميرية للطبيعة قد انحازت إلى جانب الفيروس لمنع جهودهما في توقيف عمله التخريبي الذي يعيثه في شبكات الحواسيب. وقد يؤدي حتى مجرد مسح قرص مرن ملوث من قبل بعض البرامـج الكاشفة للفيروسات إلى تفعيل المنتقم الأسود ولذا فقد كان هنالك العديد من الضحايا في الولايات المتحدة ينتظرون من فريق الأبحاث في منطقة Silicon Valley إكمال أبحاثهم على عينة البرمجة واختراع مضاد له. وعندما بدأ الزلزال واهتزت محطات عمل الحواسيب في سانتا كلارا تفاجأ الباحثان بسماع أصوات سواقات الأقراص تتوقف وشاشات المراقيب تنطفىء.

وقد قال لي McAfee لاحقاً: «لقد أسرع Ari بحمل حاسوبه النقال نوع Zenith وحملت أنا حاسوبي النقال نوع Compaq وتوجهنا مباشرة إلى بيتي المقطور الموجود في الحديقة وشغلنا حواسيبنا وتابعنا تفكيك المنتقم الأسود ومحاولة اكتشاف علاج له دون أي انقطاع. وقد أكملنا العمل خلال الليل بحيث استطعنا تحديث البرنامـج المضاد للفيروسات ViruScan ووضعه على لوح الاعلان الحاسوبي مباشرة بعد عودة الطاقة الكهربائية.

وذلك البيت المقطور والحواسيب النقالة قد استعملت أيضاً كوحدة اسعاف الكترونية في مواقع ملوثة بالفيروس حيث عملت بشكل مستقل عن الأنظمة الملوثة من أجل استرداد المعطيات.

ويجب استعمال البطاريات عند التحضير للطوارىء وابتداع طرق لاستخدامها. وقد لا تحتاج إلى مولدات للطوارىء من أجل متابعة الحوسبة لفترات طويلة عندما تنقطع الكهرباء أو تصبح غير مستقرة بسبب حالات الانقطاع أو الارتفاع الفجائي المؤقت للطاقة والتي قد تقطع عمل الحوسبة وتلحق الضرر بالعتاد.

وهنالك الآلاف من الأشخاص الذين يعيشون في مراكب ضمن الأحواض في المنطقة Bay Area ورغم أن الطاقة انقطعت عن المنازل والمكاتب على البر فإن المراكب تملك أنظمة مستقلة عاملة بالتيار المستمر (DC) ومزودة بمولدات خاصة لابقاء البطاريات مشحونة.

ولذا فإن العديد من شاشات البلدر السائل (LCD) ظلت مضاءة في العديد من الحجرات لمدة طويلة مثبتة قيمة الهاتوفات (modem) اضافة إلى الحواسيب العاملة على البطارية في حالة الطوارىء.

وضبط هاتوف الحاسوب النقال ليواصل محاولة طلب المخابرات كانت الطريقة الأكثر فعالية للاتصال عبر الهاتف بعد حصول الزلزال رغم ما بدا من التعطل الكبير في خدمات الاتصالات البعدية. (وقد أثبتت شركة الهاتف Pacific Bell أنها كانت جاهزة وقد استطاعت إعادة الخدمة من مكاتبها المركزية المحصنة ضد الزلازل في سان فرنسيسكو. والسبب الرئيسي الذي جعل العديد من الأشخاص وبالأخص خارج منطقة Bay Area، لا يستطيعون الاتصال كان بسبب الازدياد الكبير في عدد طلبات المخابرات فقد ازدادت المخابرات بنسبة 400 بالمئة وذلك لأن ردة الفعل البشرية خلال الكوارث هي الاتصال بالأحباب والمعارف للاطمئنان أو التطمين). وقد أعطيت الأولوية للمخابرات الخارجية ولهذا السبب استطاع العديد الاتصال مع خارج سان فرنسيسكو ولكن لم يستطع أحد في أجزاء أخرى من البلاد أو العالم الاتصال بتلك المنطقة. ولكن أولئك الذين فقدوا الأمل بإجراء الاتصال لأنهم لم يستطيعوا الحصول على خط لم ينتظروا الوقت الكافي، فقد يحتاج الأمر إلى عدة دقائق خلال فترة الذروة للوصول إلى مقدمة صف انتظار المخابرات. وقدرة الاحتمال المكننة للحواسيب المستعملة لطلب المخابرات تلقائياً مكنتها من تحقيق الاتصال بينما أخفق الإنسان بسبب نفاذ صبره.

وقد لعبت ألواح الاعلان الحاسوبية عدداً من الأدوار المهمة للمحافظة على الاتصالات بعد الزلزال. إذا تعطل مرفق شبكة الحواسيب أو البريد الالكتروني بسبب تلوث بالفيروس أو عمل تخريبي أو كارثة طبيعية فإن ألواح الاعلان الحاسوبية تشكل وسيلة مهمة للطوارىء، وقد ساعدت الألواح في المنطقة Bay Area بشكل خاص أولئك الذين انقطعت الطاقة عنهم بعد الزلزال ولكنهم يملكون حواسيب نقالة وهاتوفات تستطيع العمل ببطاريات داخلية أو خارجية.

وأحد الأمثلة على ذلك كانت السرعة التي استطاعت فيها شركة CompuServe إعداد نشرة خاصة بالزلزال ليستعملها إلى جانب أعضائها البالغ عددهم نصف مليون أولئك الذين يستطيعون توفير المعلومات أو يحتاجونها بخصوص الزلزال. وإحدى ألواح الاعلان الحاسوبية الأخرى The Well in Sausalito قامت بعمل جيد أيضاً مما رفع من قيمة أنظمة التحادث المحلية ولفت أنظار مجتمع الأعمال إليها عندما احتلت الصفحة الأولى في جريدة The Wall Street Journal.

وفي عدد من المناطق التي تأثرت بالزلزال حيث انقطعت خطوط الهاتف وجد مستعملو الهواتف الخلوية أنفسهم في نعمة مزدوجة نتيجة عدم انقطاع وصلات الاتصال أو إعادتها بسرعة

إلى الخدمة. وأكبر قدر من الخسائر في الاتصالات كانت بين أولئك الذين دفعوا أصلاً الكثير لنقل أصواتهم ومعطياتهم بالطريقة الأكثر فعالية، فقد تعطلت بعض المقسمات الفرعية الخاصة (PBX) لعدة أيام إما لافتقارها لنظام داعم من البطاريات أو بسبب نفاذ الطاقة الاحتياطية بعد بضعة ساعات. وقد تفاقمت مشكلتهم عندما بدأت الكهرباء بالعودة تدريجياً وبشكل متقطع وذلك بسبب وجود خطر كبير عند ترك معداتهم الكبيرة والباهظة الكلفة موصولة بالطاقة مما قد يعرضها للاحتراق بسبب الارتفاع الفجائي في الكهرباء.

وقد رسخت هذه التجربة في عقول العديد من المستعملين بحيث أنهم قاموا في خططهم بالنسبة للكوارث المحتملة في المستقبل إما بالتحويل إلى خطوط تحصل على طاقتها مباشرة من مرفق الهاتف وتجاوز المقسمات PBX الهشة أو إضافة تلك الخطوط كوسائل احتياطية داعمة. وبعد الزلزال تحولت الهواتف الالكترونية المليئة بالأزرار مجرد قطع للزينة على مكاتب المدراء بينما ظل الهاتف العادي في حجرات الهاتف في الشارع يعمل بشكل طبيعي. ولهذا السبب لا تتخلص من القارنة الصوتية إذا كنت تملكها فقد تحتاجها لنقل المعطيات بواسطة الهاتف في الشارع.

والاهتمام المتزايد في الهاتف الخلوي للاتصالات الصوتية ولارسال المعطيات كان أحد نتائج الزلزال. وحتى ولو كان الحصول على أكثر من وحدة نقالة لا مبرر له فإن الشركات الحريصة تسجل أسماء وعناوين الذين يملكون هواتف خلوية. والأشخاص الذين يملكون هواتف خلوية يشكلون أيضاً جزءاً كبيراً من مستعملي الحواسيب النقالة وقد ذكرنا كيف أن هذه المعدات تصبح مهمة جداً في الحالات الطارئة.

ويجدر بجميع الأشخاص المسؤولين عن أنظمة المعلومات الادارية (MIS) وأنظمة معالجة المعطيات أو عن أمن الحواسيب أن يعرفوا من يملك هذه المعدات في مؤسستهم ومكان وجودها. فقد يملك أحد مندوبي المبيعات نسخة عن المعطيات لم تتعرض للتلوث بالفيروس والتي يمكن استعمالها في حال عدم توفر نسخ مساندة صالحة للاستعمال كوسيلة عملية توفر الكثير من الوقت والجهد لاسترداد المعطيات.

كيف تستعيد المعطيات المفقودة؟

ويضاف إلى لائحة مستوجبات الطوارىء تفاصيل عن تصليح العتاد واستعادة المعطيات المطلوبة. وبعد الزلزال استوجب الأمر اجراء هذه الأمور كما يحصل مع أي كارثة رئيسية أو وباء فيروسي حاد في موقع محدد. وقد أثبتت بعض هذه الاجراءات أنها أفضل من غيرها.

أحد أكثر المشاكل التي تعرضت لها أنظمة الحواسيب المكتبية هي وقوعها على الأرض أو سقوط جسم ثقيل عليها مثل السقف والمصابيح على سبيل المثال. أما الحواسيب النقالة في الجهة المقابلة التي تعرضت للاهتزاز فإنها عموماً لم تتأثر كثيراً. والأقراص الصلبة في الآلات المكتبية قد تملك الكثير من قدرة المعالجة المعلوماتية ولكنها ضعيفة فيما يختص بالحالات المادية المتطلبة. ويمكن تعرض القرص الصلب للضرر عندما يتناسخ الفيروس في ملفاته ولكن الضرر الناتج في المعطيات قد لا يكون بنفس القيمة ويمكن استيعابه عند استعمال الأقراص المرنة كوسط تخزين.

وبعد الزلزال اقترف بعض الذين تعرضت أقراصهم الصلبة للضرر خطأ الاسراع بتصليح القرص عوضاً عن إعطاء الأولوية لاسترداد المعطيات الموجودة عليه. وهذا يحصل أيضاً في حالات التلوث بالفيروس فيفترض المستعمل بأن هنالك عطل عتادي بسبب سوء اداء القرص الصلب بينما الواقع هو وجود مرض في البراجيات. وفي الحالتين فإن إرسال وحدة القرص لتصليحها دون الاستعانة قبل ذلك بمساعدة خبير لتحديد عما إذا كان بالامكان استرداد المعطيات، قد يؤدي إلى فقدان المعطيات نهائياً وذلك لأنه حتى الاجراءات التشخصية المستعملة لإيجاد العطل في آلية القرص قد تتلف المعطيات.

وقدرة صمود المعطيات حتى في أصعب الكوارث بما في ذلك التلوث بالفيروس كبيرة إلّا إذا تعرض محيط عملها إلى التلف المادي. ولكن استعادة المعطيات من قبل خبراء يعرفون ما يفعلون يجب أن تتم قبل قيام العامل الفني باستعمال مقياس الدوائر ومفك البراغي، أو قبل قيام أحد الأشخاص المحدود الخبرة باستعمال براجيات قوية خدماتية أو مضادة للفيروس. وبكلمات أخرى لا تقم بإجراء عملية جراحية لدماغك إلا إذا كنت مؤهلاً لهذا العمل!

وبإمكان المؤسسات توفير الكثير من المال باستغلال قدرة تشغيل المعطيات المساندة المهمة على حاسوب نقال احتياطي أو على نظام حاسوب مكتبي مساند غير معقد نسبياً.

وقد لا تحتاج استراتيجية الجهوزية لحالات الطوارىء لأن تكون بنفس تعقيد وتطور النظام العادي. إذا تعطلت سيارتك «البورش» فلا يزال بإمكانك التنقل بسيارة الفولسفاغن القديمة!

وإذا تم التحضير بشكل جيد فإن الوظائف الأساسية للعمل يمكن متابعتها باستعمال حواسيب نقالة غير معقدة نسبياً حتى تلك التي لا تملك أقراصاً صلبة. والعديد من الأفراد والمؤسسات تملك هذه الأنظمة المكملة للأنظمة المكتبية ولذا فإنها مرافق يمكن شملها وبدون كلفة اضافية في برنامج استعادة وتعافي لحالات التلوث الفيروسية وغيرها من استراتيجيات الجهوزية لحالات الطوارىء.

وتحدد الوكالة الفدرالية لادارة الطوارىء FEMA في دليل الأعمال والصناعة للتخطيط

لحالات الطوارىء الذي تصدره بأنه ليست جميع وظائف ونشاطات الشركات مهمة بحيث تستدعي استعادة المعطيات في حالة الطوارىء. وبعض النشاطات يمكن توقيفها مؤقتاً خلال فترة الاستعادة والتعاقي، والبعض الآخر يمكن حذفه بالكامل رغم الازعاج المحتمل المترتب.

وتقدر الوكالة FEMA بأن السجلات الحيوية المهمة (الضرورية لاستمرارية العمل) تؤلف جزءاً صغيراً من السجلات الاجمالية للشركة قد لا يزيد عن 2 بالمئة. وضمن نسبة 2 بالمئة هذه قد تتواجد أحد أهم ممتلكات المؤسسة مثل المعادلات والأسرار التجارية ومناهج العمل وملخصات عن الدائنين والمدينين ومعطيات مماثلة مهمة لتجعل المؤسسة قادرة على العمل. ويمكن حفظ معظم هذه المعلومات في فسحة صغيرة جداً على أقراص حجم $3\frac{1}{2}$ بوصة والتي تعمل مع معظم الحواسيب النقالة. وبواسطة هذه المعطيات التي لا تقدر بثمن تستطيع وبقدر قليل من العناء إنشاء نسختين مساندتين تحفظ في مواقع مختلفة مع فحصها دورياً لاكتشاف أي تلوث فيروسي.

وحتى السجلات المحفوظة على أوراق مثل أوراق التأسيس وبواليص التأمين وعقود الايجار وصكوك الرهن وما شابهها من النصوص أو الرسوم البيانية غير المرقمنة يمكن مسحها بسرعة من الأوراق الأصلية وحفظها على أقراص. ومعدات المسح (Scanners) قد أصبحت فعالة وأسعارها مقبولة إلى حد تستحق فيه استعمالها لتحويل الأوراق المهمة إلى نسخ مرقمنة.

لقد جعلت حادثة الزلزال الكثير من الجهات تنتبه إلى إمكانية نسخ السجلات المهمة وحفظها في فسحة لا تزيد عن حجم حقيبة اليد.

لقد جعلت حادثة الزلزال الكثير من الجهات تنتبه إلى إمكانية نسخ السجلات المهمة وحفظها في فسحة لا تزيد عن حجم حقيبة اليد مع بقاء فسحة كافية لوضع الحاسوب النقال لتوفير المعطيات عند احتياجها.

ولقد أظهر زلزال كاليفورنيا في تشرين الأول 1989 أيضاً التغييرات الاجتماعية والديموغرافية الطويلة الأمد التي تحصل على طريقة ومكان عمل الأشخاص. وهذه التغييرات لها تأثير أساسي على كيفية تخزين ومعالجة المعطيات. وهي تؤثر على طريقة انتشار الفيروسات وعلى اجراءات الاستعادة الضرورية بعد حصول العدوى.

وكلما ازدادت وسائل الاتصال عن بعد وانخفضت نسبة العمال المتمركزين في مواقع عمل تقليدية بحيث تكون معطيات وبرامج المؤسسة منتشرة وموزعة على منطقة واسعة فإن المراقبة وبالتالي الأمان سوف ينخفضان كثيراً.. وهذا قد يزيد كثيراً من احتمال التعرض للعدوى ويعقد إجراءات الاستعادة كثيراً.

ولا توجد كارثة يمكن مقارنتها مع زلزال كاليفورنيا للعام 1989 لناحية تسببها بجعل الكثير من الأشخاص أو المؤسسات يقومون بتقييم نمط عملهم بهذا الشكل الأساسي، وأنماط العمل والاتصال والنقل التي كانت قبل الزلزال موقوفة وثابتة وواضحة المعالم يتم إعادة تقييمها بشكل جذري.

وبسبب تفاقم مشكلة ازدحام السير في المنطقة Bay Area فإن الاتصال عن بعد هو الحل الذي يجذب الكثير من الناس والمؤسسات كحل عملي لهذه المشكلة وذلك حتى بالنسبة للمدراء الذين كانوا دائماً يشكون من جدوى وجود قسم من القوة العاملة يعمل بعيداً عن مواقع المكتب المركزي.

وهنالك الآن وعي من قبل الادارات بأن وسائل الاتصال عن بعد والتخطيط لحالات الطوارىء أمران يمكن دمجهما مع استعمال الحواسيب النقالة أو المستقلة كعناصر أساسية في الاثنين. والعمال الذين يسخدمون هذه الأدوات التقنية الحديثة مثل الحواسيب النقالة والهواتف النقالة وأجهزة الناسوخ (فاكس) ومكتبات الأقراص CD -ROM والارسال الانتقالي للمخابرات والخدمات المتصلة مع الخط والاجتماعات الفيديوية وغيرها سوف يعملون بجو أفضل وأكثر فعالية ويملكون مرافق مبيتة للطوارىء عندما تضرب إحدى الكوارث المرافق المركزية للشركة.

وحالياً هنالك حوالي 30 مليون أميركي يعملون من منازلهم بدوام كامل أو جزئي وهذا العدد يزداد بحوالي مليون شخص في السنة. ومنحى العمل من المنزل قد تزايد حتى الآن في أوساط الأشخاص العاملين بشكل مستقل ولكن هذه الفكرة بدأت تلاقي رواجاً في المؤسسات الكبيرة أيضاً. وحادثة زلزال كاليفورنيا أقنعتهم أكثر بجدوى هذا الأسلوب الذي لم تكن فوائده واضحة سابقاً.

كيف تحدد المعطيات المهمة وتحميها

الخطوة الأولى في تحديد خطة الجهوزية لحالات الطوارىء هي تعريف ما هو المهم ومن ثم التأكد من سلامتها ضد جميع المخاطر التي قد تحدق بها مع وضع التلوث الفيروسي في نفس الفئة مع المخاطر الأخرى مثل الزلازل والحرائق وتدفق المياه والمواد الخطرة والزوابع وانقطاع الطاقة أو ارتفاعها الفجائي، والتخريب أو الارهاب والعواصف الرعدية والصواعق والنشاط البركاني وحتى الانفجارات النووية.

وقد تبدو الفيروسات للوهلة الأولى مماثلة للانفجارات النووية إذ قد يبدو أنك لا تستطيع القيام بأي عمل لتخفيف الأضرار الناتجة في حال أخفقت وسائل دفاعك. ولكن شركة Boeing

Aerospace بالتعاون مع وكالة وزارة الدفاع للشؤون النووية أجرت سلسلة من الاختبارات تبين كيف يمكن حماية مختلف أنواع الآلات المستعملة في المصانع بواسطة أساليب تقنية بسيطة وذلك ضد نوع من الهجوم النووي. والحاسوب الذي يشبه بالنسبة للكثير من المحترفين المصنع، يمكن حمايته ضد الفيروسات ببذل الجهد المطلوب لتنفيذ اجراءات أساسية ذات مستوى منخفض من التعقيد التقني. والفائدة الكبرى للحواسيب هي أن المعطيات خلافاً للمصنع يمكن نسخها بسهولة مما يسمح استعمال النسخة في حال تلف الأصل.

ويتضح أن المخاطر التي تقرر تغطيتها تحددها الكلفة المطلوبة. وهذه الكلفة تتمثل بالوقت والمال والازعاج المترتب والتي لا يجب أن تفوق حجم الخطر. ولكن يجب أن تقوم أولاً بتحديد المعطيات المهمة فعلاً إلا إذا كان حجم أو طبيعة العمل يحتمان تطبيق حماية شاملة على جميع المعطيات المحوسبة.

وتقترح الوكالة FEMA اجراءات تساعد على اتخاذ هذه القرارات الأولية عند تحليل السجلات المهمة. أولاً، يجب إنشاء فريق عمل من الاداريين لتحليل احتياجات السجلات المهمة للشركة كما هو مشروح في الخطوات الأربعة التالية (ومدير سجلات الشركة إذا كان هذا المنصب موجوداً هو الرئيس الطبيعي لمثل هذا الفريق.

1 ــ صنّف أعمال الشركة ضمن فئات وظائفية عريضة.

بالنسبة للمبيعات مثلاً فإن هذا يشغل الشحن والجردة. وبالنسبة للدائرة المالية فإن الفئات الوظائفية تشمل تجميع الحسابات ودفعات الدائنين وحساب الكلفة.

2 ــ قرر الدور الذي تلعبه كل دائرة في حالة الطوارىء.

ولا تكون جميع الدوائر مهمة في فترات الاستمرارية والاستعادة التي تلي الكوارث. والبعض يمكن توقيفه عن العمل مؤقتاً بينما يحذف البعض الآخر كلياً شرط أن لا يحد ذلك كثيراً من قدرة الشركة على استعادة أقسام أساسية من عملها. وجميع النشاطات التي تعتبر حيوية حسب هذه المعايير تساعد تلقائياً على تحديد معلومات الحوسبة المهمة أيضاً ولذا يجب حمايتها ضد التلوث الفيروسي وغيره من المخاطر.

3 ــ اسرد القدر الأدنى من المعلومات الواجب توفره خلال الفترة التي تلي الحالة الطارئة وذلك لضمان استمرارية الأعمال الحيوية.

وهذه المعلومات ليست بالضرورة السجلات التي تشكل الأجزاء المألوفة للأعمال الروتينية ولذا فإن التخطيط لحالات الطوارىء قد تتطلب بعض التغييرات في الإجراءات. مثلاً، توفر السيولة النقدية قد يكون مشكلة ولذا لمواصلة استلام المال لن تحتاج فقط إلى نسخ عن آخر بيان

لحسابات الزبائن أو العملاء بل تفاصيل عن طلبات الشراء والدفعات اللاحقة التي لم تسجل أو تقيد في الحسابات. والمعطيات في تقرير الجودة يجب أن لا تعكس فقط ما هو موجود في المستودع لخطة حصول الكارثة بل ما يوجد أيضاً في تقارير شبكة التوزيع ومراكز وسطاء البيع.

4 ــ حدد السجلات التي تحتوي جميع هذه المعلومات المهمة والدوائر المسؤولة عنها والطريقة الأفضل لتطبيق استراتيجية تهدف لحمايتها.

لا تعد المعلومات حيوية إذا ما تعرضت للتلوّث.

يجب اضافة محيط عمل خال من الفيروسات إلى توصيات الوكالة FEMA بخصوص الأمن وغيره من وسائل التحكم الفعلية لأوساط التخزين البعيدة عن موقع العمل. ولا يجب دخول المعطيات إلى وسط تخزين السجلات الحيوية إلا بعد اخضاعها لفحوصات التلوث الفيروسي.

وقد كان هنالك قاعدة قياسية للأمان تقول بأن المعلومات السرية تظل مهمة وحيوية شرط عدم تعرضها لأعمال التجسس والتخريب الصناعي أو انتشرت بطريقة ما. ولقد أدخلت فيروسات الحواسيب شرط آخر للأمان يصعب تطبيقه أكثر وهو يقول بأن **المعلومات لا تعد حيوية إذا ما تعرضت للتلوث** بحيث تصبح عديمة النفع أو قد تلحق الضرر إذا ما أتلفت دون علمك. والمعلومات غير الموثوق بها قد تكون أكثر ضرراً من الفقدان الكلي للمعطيات، والفيروسات قد تصبح أضرار أكثر فداحة إذا ما قامت بتغيير المعطيات بالسر وعدم إتلافها علناً.

والآن بعد أن دخلت الفيروسات في صميم حياتنا العملية لا نحتاج فقط إلى حماية المعطيات منعاً لفقدانها بل حمايتها أيضاً ضد تغييرها بطريقة قد تلحق الأذى بنا كتغيير القيم المالية في الحسابات على سبيل المثال. والمعلومات المتلفة لا تعد غير مهمة فقط بل قد تشكل خطراً على عملك. والأقراص الملوثة يجب إتلافها دائماً أي تقطيعها أو إحراقها وذلك لأن تنسيق الأقراص قد لا يكفي أحياناً لإزالة التلوث. وقد حصلت عدة حالات من تجدد التلوث بسبب عدم قيام بعض الشركات بإتلاف الأقراص الملوثة مما جعلها لاحقاً تعاود دخول النظام وتبدأ سلسلة جديدة من التلوث الفيروسي.

والملفات التي يتم تحديثها بانتظام تشكل مشكلة معينة والطريقة الوحيدة للتأكد من أن المساندة تتم بطريقة منتظمة ومنهجية هي استعمال **نظم الأسلاف**. وتتم حماية ثلاثة أجيال من الملفات حيث الملفات الأقدم هي السلف والتي تحفظ بعيداً عن موقع العمل والتي يجري تبديلها تباعاً بالأجيال اللاحقة من الملفات والتي تبدل بدورها بواسطة النسخة المساندة الأخيرة للملفات الحالية. ويجب أيضاً وجود اجراءات مضادة للفيروسات عند كل مرحلة من مراحل تغيير الجيل.

وإذا كان هنالك من درس يجب تعلمه من حادثة زلزال كاليفورنيا فهو أن تحضير نسخ مساندة هو التدبير الاحترازي الأكثر أهمية والواجب اتخاذه لتفادي مختلف أنواع الكـوارث الحاسوبية. ولا تحتاج إلى أن تكون موجود في منطقة معرضة للزلازل أو غيرها من الكوارث الطبيعية للأخذ بهذه النصيحة المهمة.

هنالك حاجة لحماية البرامـج اضافة إلى المعطيات من عدوى الفيروس في جميع الأوقات وذلك لضمان توفرها في حالة الطوارىء، وينطبق هذا الأمر بالأخص إذا ماكانت البرامـج فريدة من نوعها أو أعدت بشكل خاص لتتلاءم مع حاجاتك الخاصة. وضمان استمرارية الادارة اضافة إلى القدرة الانتاجية لجميع الموظفين هو جوهر التخطيط للجهوزية في حالات الطواريء. ولهذا فإن تقييم ما يشكل السجلات المهمة (المعطيات والبرامـج) يجب أن يأخذ العامل البشري بعين الاعتبار. أربط سجلاتك الحيوية باحتياجات أشخاصك الحيويين.

لا تثق باجراءات الوقاية ضد الفيروس والحالات الطارئة إلا إذا كنت تختبرها بانتظام

يجب اختبار جميع استراتيجيات الجهوزية لحالات الطوارىء بانتظام وتحسينها وتغييرها مع تغير الحاجات وظروف العمل. وينطبق هذا الأمر أيضاً على مخطط حماية المعطيات المضاد للفيروسات.

وقد تكون شركتك قد طورت مخططاً تنظيمياً للطوارىء للمساعدة الذاتية في جميع حالات الطوارىء مع شمل هذا المخطط الاداري لقسم يتعلق بحماية المعطيات. وإذا لم يكن الأمر كذلك فيجب الشروع بذلك فوراً.

تقوم الوكالة FEMA بإعطاء دروس تدريبية ليوم واحد ولأسبوع واحد تشدد على أسلوب توقع المشاكل خلال تقييم المخاطر وإدارة المرافق والتخطيط الأساسي لتفادي الكوارث وردات الفعل والاستعادة ومواضيع أخرى ذات علاقة.

ومن المهم معرفة كل مستعمل للحاسوب في الشركة موقعه في الاستراتيجية الشاملة لاستعادة وحماية المعطيات العائدة للشركة.

وتوصي الوكالة FEMA بتصميم برنامـج التدريب بحيث يتفاعل جميع الموظفين تلقائياً في حالة الطوارىء وبحيث يعرف جميع الموظفين الموكل إليهم مهام معينة في حالات الطوارىء مسؤولياتهم ويكونوا قد اكتسبوا الخبرة الكافية لتنفيذ عملهم بفعالية. وهذه النصيحة مهمة بالنسبة للفيروس كما هي مهمة بالنسبة للزلازل. ويجب أن يفهم الموظفون مخطط الطوارىء

بالكامل وكيف يستخدمون مهاراتهم. والأهم هو معرفة الموظفين لحدودهم ومتى وبمن يتصلون للحصول على المساعدة.

واختبار الاستراتيجية سوف يفيد الجميع كثيراً. وتستطيع استعمال أقراص تقوم بمحاكاة حالة تلوث فيروسية دون تعريض معطياتك لخطر حقيقي. ولا حاجة إلى تلويث نظامك فعلياً لاختبار وظائفه الدفاعية، مثلما لا حاجة إلى إضرام النار لاختبار وسائل اطفاء الحريق!

وسوف نشرح إجراءاً عملياً يعتمد على اجراءات اختبار برامج الحماية للسجلات الحيوية الذي أعدته الوكالة FEMA وهو يتلاءم بشكل خاص لاختبار حالات التلوث بالفيروس. أولاً، حدّد أهداف الاختبار. وسوف تحتاج على الأرجح إلى معرفة أن المعطيات الحيوية قد تم استرجاعها بأقل قدر ممكن من التوقف عن العمل بعد حصول التلوث، والتأكد من أن عملية الاستعادة تخفض احتمال تجدد العدوى إلى أقصى حد. ولهذا يجب أن يبرهن الاختبار قدرتك على استعادة السجلات:

- الحـاليـة.
- الخالية من الفيروسات.
- الآمنة من المخاطر المحتملة الأخرى مثل الكوارث الطبيعية والحرائق والسرقات وغيرها.
- وبشكل قابل للاستعمال.

وتعامل مع مهمة التحديد هذه بتحديد ما تريد فعله بالمعطيات بعد حصول الحالة الطارئة. مثلاً، قد تضطر إلى الدفع للموظفين والموردين في الأوقات المحددة ولذا فإنك سوف تحتاج إلى معرفة وضعك المادي وموقع الأموال المتوفرة. وقد تحتاج إلى تحديد حجم وقيمة ممتلكاتك ولذا يجب أن تكون معطيات حسابات القبض دائمة التحديث وسهلة الوصول. وسوف تحتاج بالطبع المحافظة على استمرارية نشاط عملك ولذا يجب توفر المعلومات المتعلقة بالطلبيات والأعمال الهندسية والانتاج وحسابات الزبائن الضرورية لمتابعة الانتاج ونشاط المبيع، بسرعة وبشكل كامل وسهل الاستعمال. وهذه المعلومات قد لا تنفع إذا ما كانت غير حديثة وبنسق الأرشفة على شريط تسجيل بحيث لا تستطيع بسهولة الوصول إليها أو معالجتها.

بالنسبة للأعمال الفردية فإن المبادىء الأساسية هي نفسها حتى ولو اختلفت التفاصيل. إذا كنت تعمل على تأليف رواية وبصدد تنقيح المسودة الثانية لتلك الرواية فإنك تحتاج إلى النسخ المساندة لتلك المسودة وليس إلى المسودة الأولى. وإذا كان العتاد المساند هو حاسوب نقال لا يستعمل سوى أقراص مرنة مزدوجة الجوانب ميكروية (حجم $3\ ^1/_2$ بوصة) فإنك لن تريد وضع النسخ المساندة على أقراص مرنة حجم $5\ ^1/_4$ بوصة.

وتوصي الوكالة FEMA بأن المعرفة المسبقة بالاختبارات يجب أن تنحصر ببضعة أشخاص فقط وقد يكون من الأفضل في بعض الحالات اجراء الاختبارات بعيداً عن موقع العمل لكي لا يتم مقاطعة روتينات العمل العادية. تأكد من أن المرافق الضرورية متوفرة مثل عتاد معالجة الكلمات.

واجعل الاختبار قريباً إلى الواقع وذلك بإعداد مشاكل معينة من النوع الذي قد يصادفه المشاركون في الاختبار فعلياً. نستطيع جميعاً تخيل ما قد يحصل إذا ما حصل حريق في المبنى ولكنه من المهم أيضاً إثبات أن مرافق الحوسبة سوف تصبح عديمة النفع في حالة الفيروس كما لو أنها أتلفت بواسطة حريق أو تدفق للمياه. وأحد مشاكل الاختبار النموذجية هي افتراض تلويث الفيروس للحواسيب في مكتب فرعي وهو ينتشر في أنحاء شبكة الشركة.

ولم يتم حتى الآن تحديد نوع الفيروس ومدى استفحاله ولكن مرافق قاعدة المعطيات الفاعلة الرئيسية للشركة قد تكون قد تلوثت ولذا لا يمكن استعمالها. ما العمل في هذه الحالة؟

ويجب أن يتحقق الاختبار من الأمور المهمة التالية:

- قدرة المؤسسة على حصر العدوى.
- توفر برامجيات اكتشاف الفيروسات المناسبة والخبرة الفنية وسهولة الوصول إليها.
- القدرة على ازالة الفيروس.
- القدرة على التعافي بحيث تعوذ الأنظمة إلى عملها المعتاد مع استرداد المعطيات التي كانت مفقودة وخلوها من الفيروسات بأسرع وقت ممكن.
- توفر مرافق مناسبة لمواصلة عمل عمليات معالجة المعطيات المهمة خلال تطبيق إجراءات الاستعادة.

التحدي الذي يطرحه هذا الاختبار هو اثبات القدرة على معاودة تشغيل العتاد وإنقاذ المعطيات المفقودة إذا ما تم التعرف على نوع الفيروس وازالته. وأحد الأجزاء المهمة من البرنامج هي إبلاغ الجميع بأن المعطيات على الأقراص الصلبة وأوساط التخزين الأخرى قد تكون ملوثة.

ولا يتوجب فقط جعل الحواسيب تعاود نشاطها مجدداً بل يجب أيضاً تزويدها بمعلومات الية نظيفة تمكنها من معاودة مهامها الأساسية. هل بالامكان دفع الرواتب في أوقاتها؟ هل بالامكان الحصول على منتوجات معينة من مصادرها وبأحسن الأسعار؟ هل بالامكان تحضير عقود التأمين؟ هل بالامكان إعداد الرسوم الهندسية والمواصفات وقائمة المواد للمنتوجات الأساسية؟ هل بإمكانك توليد بيانات جارية للمداخيل والمصاريف والأصول والخصوم؟

وقم بتعيين مدراء غير مشتركين في الاختبار للعمل كحكام، وهؤلاء الحكام لهم دور أساسي يلعبونه. يحتاجون على سبيل المثال التأكد بأن المعطيات قد أعيد تركيبها من نسخ مساندة حالية ودقيقة فعلاً وليست قديمة وغير موثوقة. ومراقبة الاختبارات الدورية من قبل المدراء ذوي الرتب العالية يساعد على المحافظة على نوعية مقبولة لإجراءات مساندة المعطيات. ومهما كانت درجة حماس الجميع في البداية فإذا لم يتم استخدام النسخ المساندة واختبارها دورياً فإن العملية سرعان ما تصبح غير دقيقة ولن تكتشف عيوبها إلّا عند حصول حالة طارئة فعلية.

التحضير للحالات الطارئة والأمان

إن المعطيات تتعرض للضرر نتيجة تدخل بشري مثل خرق طوق الأمان مثلما تتعرض لذلك نتيجة حريق أو تدفق مياه أو أية كارثة أخرى. والخطر البشري يزداد بسبب الفيروسات التي تستطيع اقتحام معظم دفاعات الأمن التقليدية ويصعب توقعها واكتشافها.

ولا يوجد شيء ثابت في حالة عمليات الحوسبة فالتغيرات تحصل طوال الوقت. وقد تحصل عن قصد عند تركيب إجراءات تشغيلية جديدة أو اعتماد برنامج تطبيقي جديد، أو قد تحصل عرضياً خلال التعديلات التي يقوم بها المستعمل. ولكن يجب عدم المساس إطلاقاً بإجراءات الأمن المتعلقة بحماية واستعادة المعطيات والمحافظة عليها بشكل متواصل وعدم إدخال التعديلات إلا بعد حصول إذن يسمح بذلك. وهذا ليس فقط لضمان عدم العبث بإجراءات الطوارىء بل كتدبير احترازي أساسي للأمان من أجل وقاية النظام من أية عملية تخريب داخلية أو لتجنب تعريضه إلى عمليات وصول غير مخولة بقصد الأذى.

وتشدد الوكالة FEMA على أن «تعديلات البرامج يجب توثيقها بالكامل مع ذكر أسماء المبرمجين الذين قاموا بهذه التعديلات ضمن مستندات توثيق البرامج. ويجب على الجهة المسؤولة عن مراقبة دائرة المستعملين ومرفق الحاسوب مراجعة تلك التعديلات والموافقة عليها قبل تطبيقها. ولا يجب السماح للمبرمجين القيام حتى بتعديلات طفيفة على برامج الإنتاج التي يشغلونها دون أخذ إذن بذلك.

وإذا كان الأمن مسألة مهمة فإن الوكالة FEMA تقترح عدداً من الأعمال الإضافية الواجب القيام بها. وهذه تشمل جعل مشغلي الحواسيب يعملون أزواجاً في جميع الأوقات حتى خلال عطلة الأسبوع والأعياد وبالأخص عند معالجة السجلات المهمة. وأحد الأساليب لذلك هي الجمع بين مسؤول أو مشغل عالي الرتبة مع شخص أقل خبرة أو حديث العهد في الشركة. واسلوب اعتماد فرق العمل له فائدة مزدوجة فهو يخفض من احتمال حصول اخطاء

أو تغيير غير مخول للمعطيات دون أن يكتشفه أحد، ويحافظ أيضاً وبشكل عام على نوعية العمل.

والموظفون الأوفياء يصلحون كمراقبين جيدين. وقد حصلت حادثة ولاية تكساس حيث لاحظ أحد الموظفين موظفاً مفصولاً من الخدمة يقوم بإعداد رسالة استقالته عند أحد المطاريف خارج دوام العمل الرسمي. وقد أبلغ ذلك الموظف المسؤولين مباشرة فتم إجراء تحقيق أدى إلى منع انتشار برنامج دودي كان قد وضعه الموظف المفصول من الخدمة وتم الحؤول دون تسببه باتلاف سجلات مهمة.

وتوصي الوكالة FEMA بتنفيذ خطوتين إضافيتين لتخفيض احتمال حصول الخطر الموجود دائماً والمتمثل بإتلاف الملفات بسبب خطأ من المستعمل أو نتيجة نية مقصودة. وهذه الأفكار المساعدة هي أيضاً تدابير احترازية مضادة للفيروسات جديرة بالاهتمام. أولاً تقوم بوضع برنامج التشغيل أو البرنامج الإشرافي التنفيذي في ذاكرة مقروءة ـ فقط (ROM). وهذا الأمر يقي مزايا حماية الذاكرة للبرنامج مانعاً التلف العرضي لقسم الملفات وكذلك الاستعمال غير المشروع للملفات. أما الخطوة الثانية فهي شمل فحوصات شاملة لتحديد اكتمال العمل في كل برنامج لضمان عدم قيام المشغلين بإنهاء البرنامج أو تركه قبل إدخال رسالة إنهاء عمل. وهذا الإجراء قد يشمل تشغيل برنامج لاكتشاف الفيروسات أو فحص مجموع، أو عمل آخر قد يساعد على اكتشاف النشاط الفيروسي.

وتقول الوكالة FEMA بأنه «يجب تدوير مهام فرق عمل الحواسيب ونوبات العمل بشكل دوري. ولا يجب على العامل معالجة نفس برامج المبرمجين لفترة طويلة من الوقت ويتوجب تشجيع المشغلين على البقاء متنبهين لأية حالات تغير في الظروف المادية للمرفق. ويتوجب قيامهم دورياً وخلال كل نوبة عمل بالانتباه إلى عدة أمور مثل القطع المغنطيسية ومفكات البراغي والمبارد وغيرها من الأدوات الصغيرة التي تشكل أدوات تخريب محتملة. وكذلك يجب الانتباه إلى معدات الأمن والإنذار بالحرائق المفصولة، والأبواب المفتوحة لغرف وحدات الأقراص المشتغلة والمعدات الطرفية المساعدة».

وتحديد جدول زمني لوقت استعمال الحاسوب يضمن استعمالاً أكثر فعالية لقدرة المرفق ويجعل من الأسهل إكتشاف حالات الاستعمال غير المسموحة لوقت الحاسوب من أجل إكتشاف عمليات نقل للملفات المعلومات المهمة (أو لإنشاء أو إدخال الفيروسات أو غيرها من البرامج المهددة للمعطيات). وتغيير جدول مواعيد عمليات معالجة السجلات الحيوية الحساسة جداً هو أسلوب احترازي معقول لحفظ الأمن بحيث لا تقوم بتشغيل البرنامج بنفس الوقت كل يوم أو في نفس اليوم من كل أسبوع. وكذلك لا يجب أن تتبع تمارين الطوارىء نفس النمط المتوقع دائماً.

وحماية المعطيات بشكلها المحوسب فعال ضد الفيروسات ولكنه لا يكفي لمنع أعمال التخريب الصناعي أو لحماية المعلومات التي قد تساعد المخرب على الدخول إلى النظام لزرع الفيروس. ولقد تكلمت مع تحري يحقق في قضية تتناول موضوع قيام مجموعة من العملاء الأجانب بإدارة حلقة لتوزيع المخدرات داخل شركتين أميركيتين كبيرتين عاملين على مبادلة الكوكايين لقاء معطيات سرية مهمة. وقد كشفت التحقيقات أيضاً بأن نفايات هذه الشركات يجري تفتيشها دائماً، وذلك لأن إيجاد المعلومات السرية من النسخ الكربونية لأوراق الحواسيب المتواصلة أو من شرائط الطابعات الصدمية أو غيرها من الاستمارات المطبوعة الملقاة في مكب نفايات الشركة قد يكون أسهل من محاولة الدخول إلكترونياً إلى النظام.

والأوساط الإلكترونية التي قد تبدو خالية من التلوث أو من المعطيات المهمة قد لا تكون كذلك. وتقترح الوكالة FEMA كتابة تتابع من الأرقام العشوائية على الأقراص وأشرطة التسجيل التي كانت تحتوي على معلومات مهمة قبل إعادة استعمالها للملفات وبرامج أخرى. وهذا قد يكون نصيحة جيدة أيضاً لإزالة التلوث بعد حصول تلوث فيروسي. وتقوم المؤسسات العسكرية بكتابة أصفار على الأقراص الصلبة الملوثة كأسلوب احترازي حتى بعدما تشير البرامج الكاشفة للفيروسات بأن البرنامج الملوث قد أزيل بالكامل. وقد يبدو الأمر وكأنه نوع من الهوس ولكن المؤسسات العسكرية تأخذ الفيروسات على محمل من الجد إلى حد التخلص من الأقراص الصلبة الملوثة. أما أولئك الذين لا يملكون ميزانية البنتاغون فلا يملكون القدرة المالية للقيام بذلك. ولكن يجب على الأقل التخلص من الأقراص المرنة التي كانت تحتوي على معلومات مهمة أو تلوثت مسبقاً. وهذا العمل هو الأفضل والأكثر ملاءمة من ناحية توفير الكلفة.

والأساليب المضادة لأعمال التخريب والموصى بها لمنع الدخول غير المسموح لخطوط إرسال المعطيات مثلاً عبر وصلات تفريع من الخطوط، قد تساعد على تخفيض التعرض لعدوى الفيروس ولكنها لا تزيلها بالكامل. ويحذر John McAfee دائماً بأن «الفيروسات تدخل الأنظمة عبر جهات صديقة». واسلوب الأمن التقليدي ليس بكاف. واعتبر هذا الوضع على أنه مماثل للمتاعب التي تتكبدها شركات الطيران خلال بعض الرحلات لضمان عدم صعود الارهابيين وعدم استعمال المسافرين البريئين دون علمهم كوسائل لنقل المتفجرات داخل حقائبهم.

وتنصح الوكالة FEMA أيضاً بالاحتفاظ بسجلات لنشاطات معالجة المعطيات كوسيلة للمساعدة على ضمان ثمامية المعطيات. وقد زودت عند نهاية الفصل الخامس نماذج مبسطة عن هذه السجلات، ولكن بالنسبة للأنظمة الكبيرة يجب أن يحتفظ المشرف أو برنامج نظام التشغيل نفسه بسجل لا يستطيع المستعملون العاديون الوصول إليه. وهذا السجل ينشيء سجل قاعدة معطيات للبرامج التي تمت معالجتها والملفات المستعملة ونشاطات المشغلين على النظام وغيرها

من العوامل، مع ربطها جميعها بوقت وتاريخ. وتسجيل الوقت الذي استغرقه نشاط الحوسبة قد يساعد على تحديد الاستعمال غير المخول.

وتنصح الوكالة FEMA بأن «يراجع المشرفون على مرفق الحاسوب وضباط الأمن في الشركة هذا السجل معاً مرة في الأسبوع على الأقل والتحقق بالأمور المشكوك بها والحالات الغير عادية».

«وبرامج الحاسوب المستعملة لمعالجة المعلومات المهمة يجب توثيقها بالكامل. وينبغي حفظ نسخة حديثة لهذا التوثيق بعيداً عن موقع العمل مع شريط التسجيل الذي يحتوي على نسخة من الملفات. والبرامج المشتراة أو المستأجرة من شركة أخرى يجب أن تحظى بنفس القدر من الحماية مثل البرامج التي تطورها الشركة».

قد تكون البرامج القادمة من مصادر خارجية قد أعدت بطريقة ما بحيث تتلاءم مع حاجات معالجة المعطيات الخاصة بالشركة. ومستندات التوثيق التي تحتوي هذه المزايا الضرورية لمثل هذه البرامج المعدة حسب الطلب قد تكون من الصعب واحياناً من المستحيل الحصول عليها من المورد بسرعة. وسياسة تشغيل مرفق حاسوب الشركة هي التي تحدد محتويات ملف التوثيق الكامل ولكن قسم البرنامج يجب أن يشمل الأمور التالي على الأقل:

- سرد واضح يصف عمل البرنامج.
- تعريف محتويات العملية.
- مخططات مبسطة لمراحل العمل أو للتسلسل المنطقي للبرنامج.
- جداول قرار.
- التشفير المصدري.
- سرد لتعليمات التجميع.
- سجل لنقاط الفحص ورسائل الخطأ وطلبات المقاطعة إلى جانب تعليمات إعادة بدء التشغيل والاستعادة.
- وصف لضوابط معالجة العمليات والدخل والخرج.

كيف تحافظ على استمرارية الاتصالات؟

يمكن استعمال جميع أوساط الاتصال الداخلية التي قد تكون استعملت لتدريب الموظفين على أساليب الحوسبة الآمنة، لإبلاغ الجميع عن خطط الاستعادة في حالات الطوارىء. وهذا الأمر يساعد أيضاً على إعادة الثقة إلى مستعملي الحواسيب في المؤسسة.

تعطيل الاتصالات المحوسبة ولذا تأكد من توفر أرقام هواتف الطوارىء للاتصالات الصوتية في جميع الأوقات.

وخط الهاتف المساعد الذي يجب أن يعرض بشكل متواصل على جميع الشاشات هو على الأرجح الطريقة الأقل كلفة لتوفير المساعدة طوال اليوم لجميع مستعملي الحواسيب في المؤسسة. والمعلومات الموجودة في الفصل السادس توفر الأساس لإنشاء خدمة الطوارىء هذه من أجل اعطاء النصائح بخصوص تشخيص حالات التلوث بالفيروس وكذلك لتوفير وسيلة اتصال للحصول على الدعم من أجل انقاذ المعطيات في الحالات الطارئة. والخط «الأحمر» قد يكون مباشر أو عبارة عن تسجيل معد لمؤسسة أو موقع معين أو لخدمة مشتركة.

وتوفر المؤسسة الدولية لفيروسات الحواسيب (ICVI) خدمة كاملة لاعطاء النصائح بخصوص الفيروسات. والنصائح القديمة عن الفيروسات عديمة النفع مثل الأخبار القديمة فالفيروس هو قصة سريعة دائمة التغيير يشترك فيها جميع مستعملي الحواسيب.

وتزود المؤسسة (ICVI) أيضاً تصاميم لإنشاء خط «أحمر» خاص يتلاءم مع كل مؤسسة على حدى. مثلاً قد ترغب بعض الشركات بشمل خدمة لدعم المستعملين من أجل البرامج التطبيقية مثل معالجات الكلمات وقواعد المعطيات، وذلك مع خدمة الفيروس. وهذا الأمر مناسب وبالأخص عند تغير الموظفين كثيراً، أو عند الارتقاء إلى نسخة أجدد للبرنامج والتي تستلزم تدريباً إضافياً.

والمعلومات المطبوعة التي تعطي تفاصيلاً عن إجراءات الطوارىء يجب وضعها عند جميع المطاريف إضافة إلى الخط الأحمر أو كبديل له. وما تريده هو ضمان قيام جميع العاملين في المؤسسة بالتصرف بطريقة منسقة ومتوقعة عند حصول طارىء. والكلفة البسيطة لتركيب وسائل الاتصال هذه التي تعطي تعليمات عن العمل الواجب القيام به في الحالات الطارئة سوف يعطي مردوده.

ويميل معظم الأفراد والمؤسسات بعد اعتمادهم سياسة شاملة ومنسقة للدفاع عن أنظمتهم ضد عدوى الفيروس هو عدم تكملة المهمة لناحية توفير الوسائل التي تمكنهم من إتخاذ الأعمال المناسبة في حال حصول العدوى. وأحد المشاكل المعينة هي ترك مسؤولية الوقاية والاستعادة لخبراء الحواسيب الفنيين لأن المشكلة تعتبر فنية محض وليست إدارية.

والحقيقة الأساسية حول فيروسات الحواسيب والتي ركز هذا الكتاب عليها تنطبق على التعافي من التلوث وغيره من الحالات الطارئة لعمليات معالجة المعطيات مثلما تنطبق على عملية الوقاية من التلوث الفيروسي. وهذه الحقيقة هي أن هذه البرامج الهدامة هي من صنع

الأشخاص والأشخاص هم الذين ينشروها إلى الآلات التي يستعملها الأشخاص الأخرين، والأشخاص هم الذين يستطيعون المساعدة عند حصول التلوث.

والفيروسات تظهر ناحية جديدة من الجهوزية للكوارث وذلك لأنه خلافاً لبقية الحالات الطارئة فإن عدوى الفيروس تظل في الخفاء لفترة طويلة جداً وقد تتطلب الحالة الطارئة الاهتمام بها قبل ظهور عوارض واضحة بوقت طويل. ولهذا فإن الجهوزية لحالات التلوث بالفيروس يجب توجيهها نحو إتخاذ أعمال سريعة وفعالة بأسرع وقت ممكن بحيث لا يتم تأخير العمل مما يجعل الوضع يتفاقم إلى درجة يتوقف فيها النظام عن العمل وتفقد المعطيات دون وجود أمل في إنقاذها.

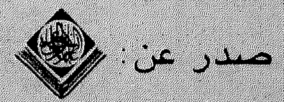
استعمل براجيات إكتشاف جيدة لتقوم بالنسبة لعملية معالجة المعطيات بعمل المكابح التي تستعملها لتوقيف السيارة وركنها إلى جانب الطريق عندما يضيء مصباح الزيت. ويتطلب هذا الأمر روتينات للطوارىء تقوم أولاً بتحديد التلوث ثم باحتوائه بأكبر قدر ممكن من مراحله الأولى وخاصة عندما تكون الأنظمة متصلة عبر شبكات.

وأخيراً سوف نكرر تشديدنا على وجوب إجراء نسخ مساندة وهو الموضوع الأساسي لهذا الفصل. والجهوزية لحالات الكوارث في عمليات معالجة المعطيات أو العمليات العامة يجب أن تكون سياستك الدائمة التي تحثك على إعداد النسخ المساندة. ومثلما تضع حزام الأمان عندما تقود سيارتك يجب أن تكتسب عادةً تحضير النسخ المساندة بحيث تشعر بعدم الراحة عندما لا تفعل ذلك كجزء روتيني من الأعمال اليومية.





صدر عن:



الدار العربية للعلوم
Arab Scientific Publishers



